2017-12

Indications and warning methodology for strategic intelligence

Kimmelman, Susann

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INDICATIONS AND WARNING METHODOLOGY FOR STRATEGIC INTELLIGENCE

by

Susann Kimmelman

December 2017

Thesis Co-Advisors: Robert Simeral
James Wirtz

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE INDICATIONS AND WARNING METHODOLOGY FOR STRATEGIC INTELLIGENCE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Susann Kimmelman	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Today's U.S. intelligence community lacks the human-centric focus needed to develop a forward-looking intelligence estimate. Using a comparative research model, this thesis explored how gray zone indicators used by the U.S. Army Special Operations Command translate into modern indicators for the intelligence community, and sought similar applications for the homeland security enterprise. The research found that, for homeland security, implementing a human-centric indications and warning methodology that focuses on the actor as the key security challenge can help provide advance warning for a planned attack or can indicate a bad actor who is inspiring others to take action.

14. SUBJECT TERMS human-centric, human domain, gray zone indicators, warning, indications	**15. NUMBER OF PAGES** 89
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

INDICATIONS AND WARNING METHODOLOGY FOR STRATEGIC INTELLIGENCE

Susann Kimmelman
Lieutenant, New York City Police Department
B.S., California State University, Fresno, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2017**

Approved by: Robert Simeral
Co-Advisor

James Wirtz
Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Today's U.S. intelligence community lacks the human-centric focus needed to develop a forward-looking intelligence estimate. Using a comparative research model, this thesis explored how gray zone indicators used by the U.S. Army Special Operations Command translate into modern indicators for the intelligence community, and sought similar applications for the homeland security enterprise. The research found that, for homeland security, implementing a human-centric indications and warning methodology that focuses on the actor as the key security challenge can help provide advance warning for a planned attack or can indicate a bad actor who is inspiring others to take action.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Today's U.S. intelligence community lacks the human-centric intelligence needed to develop a forward-looking intelligence estimate. A better understanding of homeland security challenges can come from modern indicators that inform intelligence community practitioners about emerging actors and changing situations. These new indicators must include factors about the human condition and necessitate an understanding of how people and circumstances can cause change in the world.

In an unstable situation, environmental factors and socio-political activities incentivize people to take action. Motives and conditions can cause people to act in ways that are unacceptable by societal standards, or even criminal. This call to action comes from opportunities like legal actions, strains in the economy, or changes in the sociopolitical environment.[1] By reviewing information, intelligence, and operations knowledge together, the homeland security community can discover contextual indicators that allow practitioners to evaluate "motives, conditions, opportunities, triggers, and momentum."[2]

The U.S. Army Special Operations Command is currently exploring "gray zone" indicators of bad actors; in doing so, they:

- look for signs that an actor has new or changing motives, or may act on motives.
- "apply multidisciplinary lenses to study the conditions in the operational environment, evaluating the potential energy between the mix of motives and conditions."
- look for opportunities through which can actor may gain a positional advantage.
- "measure the concentration of triggers indicating the direction and magnitude of an actor generating momentum."

[1] U.S. Army Special Operations Command, *Perceiving Gray Zone Indications* (Fort Bragg, NC: U.S. Army Special Operations, 2016), 12–13, http://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf.

[2] Ibid., 13.

- calculate the actor's momentum along a potential trajectory to determine the appropriate zone in which to alter the condition and change the trajectory.[3]

Evaluating these open-source gray zone indicators can help the homeland security community develop—or determine the appropriateness of—a modern indications and warning methodology. The U.S. Army Special Operations Command continues to develop strategic indicators for activities in the gray zone theatre, which includes a broader sociocultural framework with a "greater understanding of how we think about and visualize cognitive maneuver."[4] Social, informational, cultural, physical, and psychological elements inform intelligence collection activities and help Army strategists understand the human dynamic in the Special Operations Command battle space.

Gray zone indicators offer a set of criteria that the U.S. intelligence community can use to develop people-centric modern indicators. This research proposed modern indicators based on the gray zone indicators, and concluded that there is sufficient publicly available information to construct a modern indications and warning matrix for use in the homeland security field today.

This thesis recommends that the U.S. intelligence community adopt a more human-centric approach to intelligence collection and analysis; the approach should treat the actor—who has the capability to change the stability of an operating environment—as the main security challenge. The proposed framework examines social, cultural, political, informational, and psychological elements related to the actor. Each of these elements, compared against the actor's indicators—which include motive, conditions, opportunity, triggers, and trajectory—can begin to provide a broad picture of an emerging situation (see Table 1).

[3] Ibid., 13–14.

[4] Ibid., ii.

Table 1. Modern Indicators Matrix

ELEMENT	Social	Cultural	Physical	Informational	Psychological
INDICATOR					
Motive					
Conditions					
Opportunity					
Triggers					
Trajectory					

Possible homeland security indicators arise from each element, such as increased social media activities, sentiment analysis, availability of food, stability of food prices, directed internet searches, and demographic changes. Human-centric indicators can help intelligence professionals identify actors in an operating environment, or even identify an activity advocated for by an external party who can potentially move a person to become an actor. The homeland security field is in need of developments for indications and warnings; if strategists adopt a human-centric approach, they can use these modern indicators to mitigate future attacks and detect future actors.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the following people: Assistant Chief Jason K. Wilcox for his unwavering support during this course of study; Dr. Joseph E. Pascarella for always returning my SOS messages and sharing his insights and wisdom; my co-advisors, Robert Simeral and Jim Wirtz, for believing in this research and guiding me through to its completion; and Lauren Wollman for helping me flesh out my ideas and answering my endless emails.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION TO WARNING INTELLIGENCE

> Predictions of more sustained local and regional instability related to global economic contraction, climate change, water and food shortages, urbanization, and other socio-economic problems suggest that much of the developing world seems destined for new waves of violence that will inevitably compel the United States to act. Research provided by human geographers and other social scientists are critical to understanding international security challenges in the coming decades.
>
> —Robert R. Tomes

A. PROBLEM STATEMENT

Today's U.S. intelligence community lacks the human-centric intelligence needed to develop a forward-looking intelligence estimate. Indicators from the Cold War are no longer sufficient; nation-states and their planned movements are no longer the sole pieces of information evaluated. Today, it is necessary to incorporate a human-centric approach into intelligence collection that will facilitate a broad intelligence picture. To better understand homeland security's current challenges, decision makers must consider adopting modern indicators that can provide estimative intelligence in a rapidly changing environment. These new indicators must account for factors of the human condition, and must consider how people and circumstances can cause change in the modern world.

To provide strategic warning estimates, the U.S. intelligence community watches the movements of foreign states and their military forces to mitigate the chances of surprise attack. These estimates use information from a range of sources viewed contextually, rather than collecting and reviewing information separately and failing to develop a broader intelligence picture.[1] Strategic warning has helped intelligence operatives anticipate enemy attacks or identify developing plans to cause harm to the

[1] John Heidenrich, "The Intelligence Community's Neglect of Strategic Intelligence," *Studies in Intelligence* 51, no. 2 (2007): 11, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html.

United States and its interests, while monitoring political and social events around the world.[2]

After the Cold War, the utility of strategic intelligence diminished as policymakers sought tactical warning that detailed the events to take place, and their timing. Tactical warning calls for intelligence at the tactical and operational levels across the wider intelligence community, rather than a strategic forecast of events on the horizon.[3] Following this trend, the director of national intelligence eliminated the "national intelligence officer for warning" position in 2011.[4] Although strategic intelligence has lost its luster and value in the eyes of the intelligence community, it still performs a vital function: coordination. Indications and warning intelligence adds context to seemingly unrelated events that can signal a change on the horizon. No other form of intelligence continually monitors developments around the world as a routine function. In times of crisis, strategic intelligence signals the first warning that the enemy is preparing to take action.[5]

After the events of 9/11, critics of the intelligence community were vocal about its inability to connect the dots in a system of blinking red lights.[6] In response to this criticism, the intelligence community began to review the role of warning intelligence and its modern validity. In this this new environment of transnational threats and non-state actors, the community must meet mandates for current intelligence while also considering strategic intelligence for long-range estimates. At present, no member of the U.S. intelligence community is charged with evaluating intelligence across all elements to build a frontward intelligence estimate.

---

[2] Jack Davis, "Improving CIA Analytic Performance Strategic Warning" (occasional paper, Central Intelligence Agency, 2002), 3, http://www.dtic.mil/dtic/tr/fulltext/u2/a526569.pdf.

[3] James J. Wirtz, "Indications and Warning in an Age of Uncertainty," *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (2013): 550.

[4] John A. Gentry, "Warning Analysis: Focusing on Perceptions of Vulnerability," *International Journal of Intelligence and CounterIntelligence* 28, no. 1 (2014): 65.

[5] Cynthia M. Grabo, *Anticipating Surprise: Analysis For Strategic Warning* (Bethesda, MD: Joint Military Intelligence College, 2002), 2–3.

[6] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 1st ed. (New York: W.W. Norton, 2004), 277.

As mentioned, the intelligence methods used to gain an advantage during the Cold War are no longer sufficient to evaluate today's emerging threats. With today's fast-paced movements and posturing around the world, new indicators are needed to signal changes. Warning intelligence produces an intelligence analysis that combines information across disciplines and from multiple sources, which provides a comprehensive perspective of ongoing world events. Strategic intelligence's value now lies in the quality of new, modern warning intelligence indicators to guide decision makers.

In 2015, the U.S. Army Special Operations Command began to develop new warning indicators, focusing on the Human Domain, where the collection of intelligence is through personal interaction, by building relationships, and observing changes in the social environment.[7] For the military, these indicators are in development for operations in the Gray Zone, the space between peace and war.[8] According to the U.S. Army Special Operations Command, "Gray Zone indications will require a shift from primarily observing physical capabilities to also include seeing, assessing, and understanding the physical, cognitive, and moral frames within the strategic operating environment."[9] These new modern indicators can provide insight for intelligence strategists who are charged with monitoring non-state actors in a fast-paced international environment.

The foundation for a set of new, modern indicators begins with a framework that gathers intelligence across multiple disciplines. The new indicators must consider competition and conflict in transregional areas, and among state and non-state actors. The indicators must also be viewed in the context of specific situations that reflect regional actors' activities and conditions.[10] Accordingly, indicators must be constructed for the human domain, which the Special Operations Command describes as "the people, (individuals, group, or populations) in the environment, including their perceptions,

[7] U.S. Army Special Operations Command, *Perceiving Gray Zone Indications* (Fort Bragg, NC: U.S. Army Special Operations, 2016), 6, http://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf.

[8] Ibid., 5.

[9] Ibid., 7.

[10] Ibid., ii.

decision-making, and behavior."[11] Intelligence collection in the human domain is informed by the physical and sociocultural environment, as well as the informational and psychological sphere that shapes and changes the human domain.[12]

Gray zone indicators in the human domain go beyond the well-recognized and highly successful Cold War indicators. Today's military gray zone indicators operate under the following premises: (1) the key to security challenges in the human domain are the actors; (2) actors who are disruptive will pursue interests against the norm; and (3) actors need motive to pursue their interest in an ideology, economic view, value, or power.[13]

Sociopolitical, economic, and environmental factors provide the impetus for bad actors to take action. Motives and conditions must both be present for non-normative action. The call to action comes from opportunities through legal actions, strains in the economy, or changes in the sociopolitical environment, and begins with the actor's pursuit of his or her interests.[14] To examine contextual indicators that evaluate "motives, conditions, opportunities, triggers, and momentum," we must consider how information study, intelligence analysis, and operations knowledge converge.[15]

In exploring gray zone indicators, the U.S. Army Special Operations Command currently:

- looks for signs that an actor has new or changing motives, or may act on motives.[16]
- Applies "multidisciplinary lenses to study the conditions in the operational environment, evaluating the potential energy between the mix of motives and conditions."[17]

---

[11] Special Operations Command, *Perceiving Gray Zone Indications*, 7.

[12] Ibid.

[13] Ibid., 14.

[14] Ibid., 12–13.

[15] Ibid., 13.

[16] Ibid., 13–14.

[17] Ibid.

- looks for opportunities through which can actor may gain a positional advantage.[18]
- "measure[s] the concentration of triggers indicating the direction and magnitude of an actor generating momentum."[19]
- calculates the actor's momentum along a potential trajectory to determine the appropriate zone in which to alter the condition and change the trajectory.[20]

The areas the Army Special Operations Command is monitoring with the help of these gray zone indicators are the same areas that the wider U.S. intelligence community must monitor. Developing these indicators for use in the homeland security field would help provide a strategic outlook for decision makers. Additionally, these indicators could serve as an alarm for the intelligence community, signaling a change in world events that could affect U.S. interests.

B. RESEARCH QUESTION

> How can gray zone indicators developed by the U.S. Army Special Operations Command translate into modern indicators for the U.S. intelligence community?

Evaluating open-source datasets and global trends, including the Army's Special Operations Command gray zone indicators, can help the homeland security community develop—or determine the appropriateness of—a modern indications and warning methodology. The challenge today is to develop a warning methodology that addresses the asymmetric threat posed by non-state actors who operate transnationally. A regional global outlook of indicators to quickly and continuously evaluate information can help provide a more informed intelligence product for decision makers.

---

[18] Special Operations Command, *Perceiving Gray Zone Indications*, 13–14.

[19] Ibid.

[20] Ibid., 13–14.

C. LITERATURE REVIEW

In the early 1970s, the classified textbook *Anticipating Surprise: Analysis for Strategic Warning* by Cynthia Grabo was the standard for learning, understanding, and conducting strategic warning intelligence.[21] A warning intelligence operative's role is to watch the actions of other nations for indications of preparations to harm the United States or its interests.[22] The purpose of warning intelligence, according to Grabo, "is to enable the policymaker to make the best possible decisions in the light of the facts and judgments sent to him, and if needed to take military and political actions to counter the threatened attack."[23] As the targeted enemies of the United States move from being state armies to non-state actors, it is necessary for warning intelligence to evolve to meet the security needs of these new threats.

The intelligence community today has moved away from warning intelligence in pursuit of homeland security. Current rhetoric sees the art of warning intelligence as better suited for Cold War activities; James Wirtz notes that "because there are few mechanisms to organize and inform both intelligence professionals and government officials about their role in the indications and warning process, it is unlikely that indications and warning will see a resurgence as a key instrument of intelligence and strategic policy."[24] There are two schools of thought that inform how warning intelligence can be revised to meet the needs of today's intelligence community.[25] One school of thought, advocated by Arthur Hulnick and John Gentry, focuses on developing new collection methodologies and threat indicators. James Wirtz, advocating for the second school of thought, works within the established indications and warning framework to modernize today's warning indicators.

---

[21] Grabo, *Anticipating Surprise*.

[22] Ibid., 2.

[23] Ibid., 15.

[24] Wirtz, "Indications and Warning," 561.

[25] Gentry, "Warning Analysis," 64–65.

As early as 2005, Arthur Hulnick recognized the need to monitor for surprise attacks in a world of new, emerging threats. While the warning intelligence system in 2005 was useful, new methodologies were needed to mitigate terrorist attacks; because terrorist groups operate in small cells, the traditional indicators were ineffective.[26] Hulnick proposes using computer programs to evaluate the movements of large groups in order to detect anomalies. He also suggests evaluating terrorist targets by collecting data about the targets and searching for anomalies within the target sites.[27] Part of Hulnick's approach involves looking for terrorists who commit precursor crimes or make suspicious statements, as well as gathering intelligence from debriefings and interrogations. Finally, he states that the best warning would come from the police and private security, who may observe something in their normal course of duties, and are alert to indications of an oncoming attack.[28]

While Hulnick offers a viable solution for collecting information, the level of information he proposes collecting is at the operational and tactical levels, rather than at the strategic and policy-making levels. The proposed implementation of computer software has not yet come to fruition.[29] Furthermore, if the intelligence community is examining groups for anomalies, civil rights and privacy issues must be considered. Hulnick does not provide a method for surveilling the groups, whether inside or outside of the borders of the United States.

John Gentry also focuses on changing warning intelligence for emerging and unexpected threats. Gentry believes that by "examining both enduring and emerging warning issues can perhaps be improved by the monitoring and assessment of state and non-state actors' uses of identification and exploitation of state vulnerabilities for the purposes of both aggressive attack and target state manipulation."[30] The focus for

---

[26] Arthur S. Hulnick, "Indications and Warning for Homeland Security: Seeking a New Paradigm," *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (2005): 599–600.

[27] Ibid., 600.

[28] Ibid., 601–603.

[29] Ibid., 601.

[30] Gentry, "Warning Analysis," 65.

analysts would be to monitor perceived areas of vulnerability and the mechanisms that can influence these vulnerabilities. Focused collection activities and new measurable indicators would therefore be represented by a change in a state or group's norms.[31] Decision makers could apply Gentry's model to determine if the United States should intervene in international events, and analysts could use the model to examine the underlying factors that cause norms to change. However, Gentry does not provide a method for determining when the norms are in flux. While Hulnick and Gentry have chosen to revamp the warning intelligence methods in place, the second school of thought advocates for working within the existing intelligence framework.

As a proponent of operating within the established warning intelligence framework, James Wirtz finds warning intelligence valuable because those in a defensive alert status cannot sustain a constant posture of readiness. If there is an indication of an attack, a change in a defensive posture may be the necessary change that will deter a planned attack.[32] Similar to states, terrorists and criminals send out signals that can indicate a change; these signals can be monitored. While non-state actors can act outside of standard operating procedures issued by states, limited resources and an attempt to stay cloaked make some behaviors readily predictable and monitorable.[33] A modern warning intelligence capability begins with understanding an actors' indications of action; it does not give specific predictions. Warning intelligence can direct collection activities and analysts to specific targets when there is a belief an actor will engage in unusual activity, or when an actor is displaying unusual signals.[34] According to Wirtz, "Because small changes in defensive and law enforcement postures can deter a potential attack or produce a mission kill against initiatives launched by non-state actors, indications and warning intelligence can overcome policymakers' preferences for an 'all or nothing' response to warning."[35] Staying within the established analytical framework, Wirtz

[31] Gentry, "Warning Analysis," 66–67.

[32] Wirtz, "Indications and Warning," 553.

[33] Ibid., 555–556.

[34] Ibid., 558–559.

[35] Ibid., 560.

provides a shift in warning signals to meet today's homeland security setting. While states can still utilize warning intelligence, the focus can easily transition to monitoring non-state actors.

Today, the responsibility for indications and warning intelligence rests with the individual members of the National Intelligence Council. While the intelligence community does not place importance on warning intelligence, this type of intelligence provides an all-inclusive perspective that incorporates elements from all aspects of the community. Much like the literature today, the discussion of warning intelligence predominantly compares the events of 9/11 and the attack on Pearl Harbor. After much criticism of the intelligence community and its failure to stop the 9/11 attacks, the focus is again on the role of intelligence in the homeland security enterprise. Only in the past five years has there been a resurgence in literature that investigates the role of warning intelligence and its modern applicability. This reemergence has been limited to discussions about the probability of developing new warnings and indications within the intelligence community, while the U.S. military has been developing modern indicators for use in gray zone conflicts.

D. HYPOTHESIS AND ASSUMPTIONS

This thesis begins with the assumption that there are currently a relevant number of open-source materials that can contribute to the development of a modern indicator methodology. The U.S. intelligence community's most successful indicators were during the Cold War era, when there was opportunity to evaluate the adversary's every movement and produce an informed intelligence estimate for decision makers. Since the Cold War era, the intelligence community has relied on technological advances to keep up with the faster pace of society and the growing need for a broader intelligence estimate. Images are now retrieved from unmanned aerial vehicles that can travel further into hostile environments and provide more precise images, versus low-contrast images from orbiting satellites. Intelligence today is gathered from Global Positioning System signatures embedded in social media applications and posted in open sources that are

available for review. Electronic signatures today are collected from cellular networks, and public spaces are easily searched using crowd-sourcing software.

Margolis noted that the Central Intelligence Agency "employ[s] several intelligence gathering methods which utilize human, signals, geospatial, measurements and signature intelligence," but operations conducted in the absence of or based on faulty human intelligence have resulted in the agency's greatest failures.[36] Today's intelligence disciplines lack the capacity to monitor for sociocultural intelligence, described by Tomes as "the nature of intelligence and knowledge requirements that policymakers seek as input decisions about preferences, ideology, behaviors, affiliations, and perceptions of individuals and groups."[37] Rather than relying strictly on data and imagery, the U.S. intelligence community must consider a population-centric approach to guide the nation's strategic intelligence and inform national security policy.[38]

The U.S. Army Special Operations Command understood that warnings and indicators that were successful during the Cold War cannot keep pace with today's regional threats and non-state actors.[39] Accordingly, the command began developing strategic indicators for activities in the gray zone, which operates in a broader sociocultural framework with a "greater understanding of how we think about and visualize cognitive maneuver."[40] The U.S. Army Special Operations Command now considers social, informational, cultural, physical, and psychological elements when forming an understanding of the human dynamic in its operational space.

The U.S. intelligence community has a similar need to develop modern indicators by exploring sociocultural implications in the human domain to meet today's homeland security challenges. One example is the migration of Muslim ethnic minority residents

---

[36] Gabriel Margolis, "The Lack of HUMINT: A Recurring Intelligence Problem," *Global Security Studies* 4, no. 2 (2013): 44.

[37] Robert R. Tomes, "Toward a Smarter Military: Socio-Cultural Intelligence and National Security," *Parameters* 45, no. 2 (Summer 2015): 63, https://ssi.armywarcollege.edu/pubs/parameters/Issues/Summer_2015/9_Tomes.pdf.

[38] Ibid., 69.

[39] U.S. Army Special Operations Command, *Perceiving Gray Zone Indications*, 7.

[40] Ibid., ii.

(Rohingya) from Myanmar to refugee camps in Bangladesh. The Arkan Rohingya Salvation Army, now designated a terrorist group by the Myanmar government, is being held responsible for attacks against the military and police bases. In response, the Myanmar government has deployed security forces that have been accused of excessive use of force and human rights violations. More recently, the activities in the region have come under the scrutiny of the United Nations.[41] A second example is Germany's call for a nuclear European Union, vocalized after the election of U.S. President Donald J. Trump. This call to arms has reintroduced the idea of a nuclear arsenal as a deterrent against Russia; white it comes from the fringes of German society, it remains an area that needs continuous monitoring for persons that may want to create a situation for Germany to arm itself and the European Union.[42] Neither situation—Myanmar or Germany—directly affects the United States, but the U.S. intelligence community still has a need to monitor for potential actors; potential actors can call on others to take action, causing events that can change a region's stability.

The focus of this thesis is the need to develop modern warning indicators so the U.S. intelligence community can better inform decision makers. This thesis suggests that it is possible to leverage today's technologies for elements of the human domain using open-source information. This information can be collected and analyzed for population-centric intelligence that can provide context for global and regional activities. The U.S. Army Special Operations Command now uses five indicators to inform its operations in gray zones. This thesis proposes that these same indicators can be developed to help the intelligence community formulate foreign policy and better inform decision makers.

E. RESEARCH DESIGN AND METHODOLOGY

This study was approached using the comparative research model. The Army's Special Operations Command gray zone indicators offer a set of criteria that the U.S.

41 Lynn Kuok, "While the World Sleeps, Myanmar Burns: The Latest Rohingya Crisis," *Foreign Affairs*, September 28, 2017, https://www.foreignaffairs.com/articles/burma-myanmar/2017-09-28/while-world-sleeps-myanmar-burns.

42 Ulrich Kuhn and Tristan Volpe, "Keine Atombombe, Bitte: Why Germany Should Not Go Nuclear," *Foreign Affairs* (July/August 2017): 103–104.

intelligence community can use to develop people-centric modern indicators. The focus of this study is to explore the available open sources of information to determine if modern warning indicators can be constructed in the intelligence community to parallel those implemented by the Army's Special Operations Command.

This study is limited to warning indicators used to produce strategic intelligence. This research does not focus on tactical or operational intelligence. The indicators were developed by evaluating current gray zone indicators used by the U.S. Army Special Operations Command in the human domain. The study considers the availability of resources to provide information about actors, the environmental stimulus and opportunities for the actor, and what triggers the actor to take action. The research was conducted based on the public availability of open sources, or sources that are accessible at a nominal cost.

F. CHAPTER OUTLINE

This thesis is organized into four chapters that explore the history of strategic intelligence, the gray zone indicators, and consideration for a methodology to construct modern day indicators. Chapter II reviews the rich history of strategic intelligence in the U.S. intelligence community, as well as the foundations of the gray zone indicators. Chapter III explores the availability of open sources and what people-centric information these sources provide. Chapter IV compares the indicators that have worked in the gray zone and the compatibility to construct modern indicators with open sources for use today.

II. THE EVOLUTION OF THE INDICATIONS AND WARNING FUNCTION IN THE U.S. INTELLIGENCE COMMUNITY

> Anyone who is to start military operations in one part of the country should know the condition of the country as a whole. To start such an operation without such knowledge is to court defeat regardless of whether it is a defensive or offensive operation.
>
> —Ku Tsu-yu

In the past, governments understood their enemies to be other nations and interacted with their adversaries as whole nations. Today, the U.S. government must prepare itself for diverse domestic and foreign threats (e.g., biological, military weapons, or suicide bombers) from both nations and non-state actors. In a changing world, policymakers require different types of intelligence. To understand strategic intelligence today, we must first understand its evolution, and how indicators and warnings have guided U.S. government actions in the past.

A. STRATEGIC INTELLIGENCE

The methodology behind strategic intelligence involves conducting intelligence analysis, communicating future threats to national security teams, and preventing surprise attacks. To this end, strategic warning orients national decision makers to emerging threats, and provides assessments of global events that can affect national security.[43] Policymakers must continually evaluate the nation's readiness to face these threats. Strategic intelligence provides the knowledge needed to make decisions and implement policies.[44] With the correct information, leaders can better frame the course of action and predict how other nations will react. Before making decisions, policymakers must consider how others view U.S. policy, how other countries may counter U.S. policy, how other countries may deploy defensive tactics, and how to mitigate vulnerabilities created

[43] Davis, "Improving CIA Analytic Performance."

[44] Ibid., 2–3.

by selected policies.[45] The decision makers must consider dangers to national security, and must identify opportunities to advance U.S. foreign policy.[46]

In the post-9/11 intelligence community, analysts responsible for indications and warning intelligence utilize all sources of information, guidance from subject-matter experts, and specialized tradecraft to prepare an intelligence estimate. This intelligence helps the policymaker prevent harm or limit damage to the United States and its interests.[47] Jack Davis, of the Sherman Kent Center, defines the goal of strategic warning as "analytic perception and effective communication to policy officials of important changes in the character or level of security threats that require re-evaluation of U.S. readiness to deter, avert, or limit damage—well in advance of incident-specific indicators."[48] The related analysis takes diverse elements into consideration, including threats, economic fluctuations, civil unrest, or any incident that could result in a change to the status quo.[49]

The role of strategic intelligence differs from the roles of tactical and operational intelligence. Tactical warning intelligence focuses on specific events that can harm U.S. interests, such as military or terrorist attacks.[50] Erik Dahl describes tactical intelligence as the preparation to engage in operational activities.[51] Operational intelligence evaluates targets and combatants; it explores the enemy's vulnerabilities, as well as the critical infrastructures that can destabilize the enemy through kinetic activity. Although operational intelligence supports operational planning, it does not produce the actual plans for tactical execution. Tactical operations may undergo a post-event evaluation

---

[45] Davis, "Improving CIA Analytic Performance," 3.

[46] Jack Davis, "Strategic Warning: If Surprise Is Inevitable, What Role for Analysis?," *Kent Center Occasional Papers* 2, no. 1 (January 2003), 3, https://www.cia.gov/library/kent-center-occasional-papers/vol2no1.htm.

[47] Ibid., 1.

[48] Ibid., 3.

[49] Ibid., 5.

[50]Ibid., 3.

[51] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and beyond* (Washington, DC: Georgetown University Press, 2013), 22.

process to determine their effectiveness.[52] While operational and tactical intelligence are concerned with activities happening in the present, strategic intelligence focuses on the long-range monitoring and analysis of possible future events that can change or disrupt world order.

B. ANTICIPATING SURPRISE

Strategic intelligence has evolved; whereas past analysts monitored world events, current analysts evaluate a wide variety of information for possible indicators. The most authoritative work on strategic warning has come from Cynthia Grabo, whose seminal manual, *Anticipating Surprise: Analysis For Strategic Warning*, has recently been declassified.[53] According to Grabo, warning intelligence is largely measured by:

- Direct action by hostile states against the United States or its allies, involving the commitment of their regular or irregular armed forces.
- Other developments, particularly conflicts affecting U.S. security interests in which hostile states are or might become involved.
- Significant military action between other nations not allied with the United States.
- The threat of terrorist action.[54]

A warning can be a threat that directly affects the United States, or a threat of confrontation involving other nations. Warning intelligence analysts must continuously scan for events on the horizon and ongoing international developments that indicate a hostile action against the United States or its interests. Warning intelligence serves a dual purpose: it continuously monitors ongoing events, and informs available options for times of crisis. In a crisis, warning intelligence is the alarm that sounds when an adversary makes a move, and the source of possible actions needed to counter the threat.[55]

---

[52] Joint Chiefs of Staff, *Joint Intelligence*, JP 2-0 (Washington, DC: Joint Chiefs of Staff, 2013), I24–I25, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

[53] Grabo, *Anticipating Surprise*.

[54] Ibid., 2

[55] Ibid., 15.

Warning intelligence relies on indicators that point to changes or developments of possible significance. Although they do not provide complete certainty, indicators may provide insight into how an adversary will act or react. Indicators help analysts determine if the government should anticipate hostile activities.[56] Warning intelligence does not provide information that can be validated with certainty; it examines a series of indicators in order to draw logical conclusions. Warning intelligence's validity can only be evaluated after the fact. The best warning product is therefore one that develops over time, when a situation is continuously reviewed and the enemy's practices are continuously monitored.[57]

Warning intelligence, at its best, produces an educated prediction. Policymakers must understand that its output is estimates rather than certainties. The analyst must evaluate not only the enemy's capabilities, but also their intentions and possible actions. The analyst must then articulate the reasoning behind the estimate to the decision maker to facilitate an informed decision.[58]

C. THE EVOLUTION OF STRATEGIC INTELLIGENCE

Strategic intelligence in the American intelligence community began shortly after World War II when the United States recognized its poor preparation for threats at the onset of the Cold War. By 1948, the Central Intelligence Agency (CIA) employed several analysts to illuminate Communist countries' possible next moves, based on their indications.[59] Cynthia Grabo defines an indicator list as "a compilation of projected, anticipated or hypothetical actions which any nation might take in preparation for hostilities or other inimical actions."[60] At the same time, the military established a Joint

---

[56] Grabo, *Anticipating Surprise*, 3.

[57] Ibid., 5–6.

[58] Ibid., 14–15.

[59] Cynthia M. Grabo, "The Watch Committee and the National Indications Center: The Evolution of U.S. Strategic Warning 1950–1975," *International Journal of Intelligence and CounterIntelligence* 3, no. 3 (1989), 365–366.

[60] Ibid., 365 (footnote).

Intelligence Indications Committee, which produced a weekly report that circulated among senior government officials.[61]

In 1951, the Joint Intelligence Indications Committee was determined to be the nation's lead agency in strategic intelligence; it was renamed the Watch Committee, the name used by the CIA's strategic analysts. In 1954, the Watch Committee received formal recognition as the National Indications Center, with a full-time professional staff comprising members of various intelligence agencies. The National Indications Center director came from the CIA, but still operated from office space in the Pentagon. The role of the Watch Committee expanded from examining strictly military threats to include examining how the Communists could exploit situations or create other threats.[62]

The Watch Committee had to cut through its share of bureaucratic wrangling and red tape. The committee also had to work against traditional intelligence analytic methods to produce estimates, which led to obstacles in producing timely warnings. According to Grabo, these obstacles included:

- Over-reliance on order of battle "proof" to assess mobilization and deployment of units.
- Slowness to reallocate analytic resources in new situations ([e.g.,] failure to assign analysts specifically to examine mobilization not just order of battle).
- Reluctance to accept readily available unclassified information as too "low grade."
- Over-reliance on classified sources even when they are not productive.
- Excessive preoccupation with current data at the expense of longer-term basic research.
- Dismissal of public statements and decrees as "mere propaganda."
- Reluctance of current and military "experts" to consider the alternative views of indications specialists.

---

[61] Grabo, "The Watch Committee," 366.

[62] Ibid., 369–370.

- Reluctance to alarm senior officials with unpleasant information, particularly when it is not yet proven.[63]

Over time, the Watch Committee grew less effective. Analysts were forced to issue diluted versions of their estimates in favor of unanimity with other intelligence agencies. The intelligence product did not convey competing analyses of events. The committee's restricted activities resulted in fewer incidents that could be assessed as warning problems.[64] The intelligence community eventually became better organized and established its own watch officers, who could easily set up task forces for emerging issues. In March 1975, the Watch Committee and the National Indications Center were disbanded. Their members were transitioned into a smaller unit, the Strategic Warning Staff, whose focus was on long-term indicators and warning issues. The Strategic Warning Staff eventually evolved into the staff for the National Intelligence Officer for Warning.[65]

In May 1979, the director of central intelligence established the National Intelligence Warning System to assist with warning intelligence duties. The system was established under the Director of Central Intelligence Directive No. 1/5: *National Intelligence Warning*. The directive begins with two definitions:

> A) *Warning* as used herein encompasses those measures taken, and the intelligence information produced, by the Intelligence Community to avoid surprise to the President, [National Clandestine Service], and the Armed Forces of the United States, by foreign events of major importance to the security of the United States. This includes strategic, but not tactical warning.
>
> B) *Strategic Warning* is intelligence information or intelligence regarding the threat of the initiation of hostilities against the U.S. or in which U.S. forces may become involved; it may be received at any time prior to the initiation of hostilities. It does not include tactical warning.[66]

---

63 Grabo, "The Watch Committee," 377.

64 Ibid., 383–384.

65 Ibid., 385.

66 Stansfield Turner, *National Intelligence Warning*, Director of Central Intelligence Directive 1/5 (Langley, VA: CIA, 1979), 1, https://fas.org/irp/offdocs/dcid1-5.html.

Tactical warning is warning received at any time after hostilities start. The deputy director of central intelligence oversaw the National Intelligence Warning System.[67]

The analyst assigned to the national intelligence officer for warning position oversaw the analysis of all intelligence sources that could provide warning. This meant the analyst was responsible for evaluating competing analyses within the intelligence community and determining if it was necessary to issue a warning.[68] The national intelligence officer for warning was also the chair of the Warning Work Group, which helped coordinate warning activities within the intelligence community. Each member of the intelligence community was responsible for implementing a structure to facilitate the warning mission and support the National Intelligence Warning System.[69] Like many other intelligence community roles, the role of strategic intelligence (through the use of warnings and indicators) has been criticized. Critical evaluations over the years have affected the way the intelligence community operates, and have highlighted points of consideration for the community.

D. CHALLENGES OF STRATEGIC INTELLIGENCE

The classic work on warning intelligence is Roberta Wohlstetter's examination of signals before the attack on Pearl Harbor on December 7, 1941.[70] In her analysis, Wohlstetter acknowledges that there was sufficient warning intelligence before the attack to signal policymakers' need to act. The signals, however, were distributed among various military personnel and decision makers, none of whom received all the related information at any given point in time.[71] Wohlstetter cites several factors that led to the surprise at Pearl Harbor, including a cumbersome bureaucratic organization that did not equally share information with its counterparts (i.e., Army and Navy), the ambiguous wording of the messages sent by the Japanese, and misinterpreted messages. The most

---

67 Turner, *National Intelligence Warning*, 1.

68 Ibid., 2.

69 Ibid., 3.

70 Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

71 Ibid., 384–385.

commonly referred-to finding in Wohlstetter's work is overabundant noise that drowns out the important signals. When analysts and decision makers surrounding Pearl Harbor received an overwhelming flow of information, they were unable to distinguish between true intelligence and irrelevant information.[72]

Just one year after the events of 9/11, Jack Davis evaluated how CIA analysts could improve their performance in the area of strategic warning. Davis summarized strategic warning as a method to prevent surprise by advising policymakers about the likelihood of harm to U.S. interests. For strategic warning to be effective, it is necessary for analysts not only to report their conclusions, but also to interpret them (i.e., to determine a threat's plausibility). The analyst must also draw policymakers' attention to issues they have not yet considered, but that may need to be in the future.[73]

Davis reviewed post-mortem critiques of warning intelligence outputs and found that analysts often fail to evaluate alternative actions when testing assumptions in a final product. He also found that analysts needed to consider denial and deception more often when making analytical judgments. Davis saw a particular, two-pronged role for warning intelligence analysts: their first role is to help the government prepare for an emerging threat, and their second role is to establish possible actions to mitigate or minimize the threat.[74]

When reviewing the role of warning intelligence, Fred Borch compared the events of 9/11 to the bombing of Pearl Harbor.[75] He first comments that Pearl Harbor was a military target by military force, while the 9/11 attacks were perpetrated by criminals who had predominantly civilian targets.[76] In reviewing the events of 9/11, he did not find that the United States was unprepared for a precisely planned attack with precision

---

[72] Wohlstetter, *Pearl Harbor*, 389–395.

[73] Davis, "Improving CIA Analytic Performance," 3.

[74] Ibid., 8.

[75] Fred L. Borch, "Comparing Pearl Harbor and '9/11': Intelligence Failure? American Unpreparedness? Military Responsibility?," *The Journal of Military History* 67, no. 3 (2003): 845–860, http://www.jstor.org.libproxy.nps.edu/stable/3397329.

[76] Ibid., 846.

execution. The terrorists took advantage of U.S. technological vulnerabilities, seeing the airlines as a minimally fortified method of travel.[77] Borch concluded that the events on September 11, 2001, were not the result of failed intelligence collection or early warning.[78] He reasoned that if the law prohibited the CIA and Department of Defense from collecting information, then an attack planned and carried out in the United States would not have been detected by either agency. The proper investigative body within U.S. borders was the Federal Bureau of Investigation (FBI), which did not focus on conducting counterterrorism investigations. The CIA had collected intelligence activities from around the world and placed individuals on a watch list, but had no substantive indications of an attack on U.S. soil that would originate inside U.S. borders.[79]

Borch recognized that there was much more information available to those guarding against the Pearl Harbor attacks, but concluded that there was no warning or indications that an attack was imminent on American soil before Sept 11, 2001. Borch further defended his position by recognizing that the agencies charged with the intelligence function were acting within the scope of the law; there was nothing further that could have been done to warn of the planning or carrying out of the 9/11 attacks.[80]

Bowman H. Miller positions warning as a key part of intelligence for both the producer and the consumer.[81] Strategic warning begins with assumptions that activities are routine and carried out in the same manner. The surprise attack is worrisome to policymakers and the intelligence community needs to forewarn policymakers about these types of events.[82] When analysts cannot determine an actor's intentions or possible course of action, they cannot distinguish anomalies. Nevertheless, intelligence analysts should anticipate the information decision makers need and forecast future threats.[83]

---

[77] Borch, "Comparing Pearl Harbor and 9/11," 857.

[78] Ibid., 860.

[79] Ibid., 853.

[80] Ibid., 853–854

[81] Bowman H. Miller, "U.S. Strategic Intelligence Forecasting and the Perils of Prediction," *International Journal of Intelligence and CounterIntelligence* 27, no. 4 (2014), 688.

[82] Ibid., 689.

[83] Ibid., 692.

Decision makers must understand that warning intelligence cannot determine the precise likelihood of an event; rather, it analyzes possible foreign activities, and recommends responses and policy alternatives.[84] Miller concludes that while warning intelligence is not perfect, it does identify and monitor important indicators that can signal changes in strategic value, whether in the homeland or abroad.[85]

E. STRATEGIC FAILURE OR BAD POLICY

The attack on American soil on September 11, 2001, led to one of the largest reviews and reforms of the U.S. intelligence community. *The 9/11 Commission Report* is perhaps the best-known review of the 9/11 events; it offered a scathing assessment of the American intelligence community's failure to prevent the attacks.[86] In Chapter 8, "The System Was Blinking Red," the 9/11 Report goes on to document the information and intelligence that was gathered by various members.[87] The assessment begins by counseling that reporting must alert all intended recipients about intelligence estimates. The 9/11 Commission recognized, however, that the president and senior government officials received only select pieces of intelligence due to the volume of reporting.[88] The report concluded the following:

> The September 11 attacks fell into the void between foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign—but from foreigners who had infiltrated into the United States.[89]

---

84 Miller, "U.S. Strategic Intelligence Forecasting.", 694.

85 Ibid., 699.

86 National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*.

87 Ibid., 277.

88 Ibid., 254.

89 Ibid., 263.

The 9/11 report documents that U.S. government decision makers received many sources of intelligence. It show that, month after month, the intelligence community had additional information and intelligence to give at least a hint of an attack on the horizon. Nevertheless, due to restrictive policies, including the domestic–foreign dichotomy in intelligence collection and analysis and bureaucratic red tape, those who could have used the intelligence to further their investigations did not receive it. It is easy to identify this as an intelligence failure, but the American intelligence community could only operate within the boxes drawn for them.

The U.S. government as a whole failed to see a new emerging threat of transnational actors and non-state actors, and how ill-prepared the American law enforcement and intelligence communities were when it came to dealing with this threat. Amy Zegart attributes the intelligence community's failures to its inability to adapt after the Cold War.[90] She links these failures to cultural pathologies that did not embrace new technologies or methodologies, and the new problem space. The community's failures can also be attributed to poorly incentivized promotions, and the longtime weaknesses in FBI and CIA operations.[91] Zegart also advocates that the intelligence community was made aware of its shortcomings in the many reviews and commissions, but failed to make fundamental changes.[92]

Erik Dahl argues for warning that is beyond strategic. Warnings and indicators give a sweeping view of what may take place in the future, but they lack specifics for engagement.[93] He believes that there were many reports and briefs before 9/11 and a growing concern over a terrorist attack by al Qaeda. Nevertheless, many of warnings were not specific and did not refer to an imminent plot. The intelligence community could have made an effort to present the intelligence in different formats, but the result

---

[90] Amy B. Zegart, *Spying Blind* (Princeton, NJ: Princeton University Press, 2009), 3.

[91] Ibid., 4.

[92] Ibid., 12, 16–17.

[93] Dahl, *Intelligence and Surprise Attack*, 129.

would have been the same; there was nothing specific that would have prompted the government to take action.[94]

Dahl argues that decision makers do not take action based solely on strategic warning. Rather, he suggests there should be specific intelligence—what he calls tactical warning. He further states that, in addition to receiving specific intelligence, the decision maker must be receptive to the intelligence and feel as though the threat is grave enough to warrant action.[95] In reflecting on 9/11, Dahl makes the following argument:

> Given the intelligence warning available and the lack of receptivity among policymakers, it is very unlikely that greater imagination among intelligence officials could have prevented the 9/11 attacks. Senior policymakers did not truly believe that terrorists might use commercial airliners as aerial bombs. The possibility has been imagined and numerous government officials had been warned. But because no such attack had ever occurred before, these warnings were seen as little more than imaginative scenarios, and little action was taken against the threat.[96]

While the failure to stop the 9/11 attacks has been blamed on policymakers and the U.S. intelligence community, Dahl argues that there was no tactical warning that could have indicated an imminent threat. Without such a warning, it is difficult to convince decision makers to take action.

Tactical intelligence is an important call to action for decision makers, and it functions differently from strategic intelligence. The work of strategic intelligence identifies nations' or actors' movement that alert the government to changes in the status quo. The function is to sound the alarm, if necessary, that the decision maker may have to be prepared to take action, whether by diplomatic notice or military defensive posturing; this signals that the decision maker must take the time to review the options and how they will be received. When the government is in the realm of tactical intelligence, the threat on the horizon is no longer a probability; it necessitates the government's immediate action to stop harm to its citizens, assets, and interests.

---

[94] Dahl, *Intelligence and Surprise Attack*, 129.

[95] Ibid., 154.

[96] Ibid., 159.

F. MODERN-DAY INDICATIONS AND WARNING

In recent years, the luster of strategic intelligence has begun to dull. During its prime in the Cold War, strategic intelligence methodically tracked the movements of troops, the shipments of armaments, and the raw materials a country was stockpiling. The enemy was a known country that the intelligence community studied and monitored for a discrete period. The methodology was slow paced, but there was time for continued reviews and adjustments to proposed intelligence estimates. When strategic intelligence was in its infancy, analysts worked to compile indicators to assist in their mission of determining what helped to signal an impending change.[97]

Today there are two schools of thought on how warning intelligence can meet the intelligence community's needs (as discussed previously in the literature review). First is the development of new indicators. While it may be plausible to create new warning indicators in the post-9/11 environment using a new computer program designed to detect behavioral anomalies, this technology at present does not exist.[98] Another method is to track anomalies in a group that indicate preparations to cause harm to a state. This method, however, captures only one aspect of the warning indicators needed today to monitor regional and transnational threats of non-state actors.[99]

A second school of thought advocates for working within the existing intelligence framework. Newly developed indicators would direct collection and analysis activities. A modern warning intelligence capability begins with understanding actors' indications of action and does not give specific predictions.[100] Only in the last decade has resurging literature investigated the role of warning intelligence and its applicability to the intelligence community in a time of fast-paced movements and with the necessity to monitor non-state actors.[101]

---

97 Grabo, *Anticipating Surprise*, 3.

98 Hulnick, "Indications and Warning," 599–600.

99 Gentry, "Warning Analysis," 65–67.

100 Wirtz, "Indications and Warning," 553.

101 For a full discussion, see the literature review.

In 2011, former Director of National Intelligence James Clapper placed responsibility for warning on the entire National Intelligence Council.[102] While warning intelligence is the duty of each member of the intelligence community, strategic intelligence provides a global outlook that interacts with every part of the intelligence cycle. Current discussion about warning intelligence compares the events of 9/11 and the attack on Pearl Harbor, but has not spent much time exploring how to develop new indicators or discussing the necessity of a strategic outlook for world events.

Cold War indicators are no longer relevant today, but analysts have an opportunity to build up indicators to produce strategic intelligence. Indicators provide a glimpse into the direction that the enemy may proceed to cause harm. When any of the anticipated activities within indicators occur, they are an indication of possible change.[103] Today's overabundance of open-source information and access to worldwide audiences through social media will challenge analysts who are attempting for form new, modern indicators.

As with the formulation of warning indicators during the Cold War, to create new, modern indicators, analysts will need to understand that some activities are readily visible and can send indications of change on the horizon, while other indicators are small, unrecognizable movements. These latter indicators develop slowly and methodically, and are often tailored to the specific group or geographic region monitored. Analysts will also need to consider activity on social media and open websites, as well as activities planned through encrypted sources. It will not be easy to establish new indicators, but the implications for homeland security make the task worthwhile.

---

[102] Gentry, "Warning Analysis," 65.

[103] Grabo, *Anticipating Surprise*, 2.

G. STRATEGIC INTELLIGENCE AND THE NEED FOR WARNING

In one of the greatest military strategy books written, Sun Tzu offers the following guidance:

> Generally, he who occupies the field of battle first and awaits his enemy is at ease; he who comes later to the scene and rushed into the fight is weary. … Therefore, determine the enemy's plans and you will know which strategy will be successful and which will not.[104]

The pace of modern life and its information overload can be overwhelming for the average person, and even more so for those charged with evaluating information as potential intelligence for national security. However, it is still necessary to analyze information for its relevance and usefulness in securing the homeland and protecting U.S. interests.

Strategic intelligence provides decision makers with intelligence estimates regarding possible future actions. Strategic intelligence analysts provide alternative courses of action to help decision makers understand how U.S. policy may be received, and offer guidance about how other countries may react to the possible course of action. The guidance provided is not mystical; it is based on research, analysis, cultural understanding, and the evaluation of ongoing world events.

Strategic intelligence provides a broad picture of what is shaping the world, and how it could change. Those who conduct strategic analyses also evaluate information and intelligence at all points of the intelligence cycle; they do not wait for finished products to evaluate how their analysis fits into the broader world perspective. Beyond the policy implications, however, strategic intelligence is the voice of warning that signals a change in the status quo that requires immediate attention.

To heed Sun Tzu's general war strategy, the government should always have a warning system in place, especially when concerning matters of homeland security. At present, each member of the intelligence community is expected to be on watch for an impending attack. No entity, however, oversees and integrates intelligence from the

---

[104] Sun Tzu and Samuel B. Griffith, *The Art of War* (London: Oxford University Press, 1971), 96–100.

various agencies to develop a full view of world events that could impact the United States and its interests. It is much too simple to say that there is a "failure to connect the dots."[105] While members of the intelligence community are capable of establishing warning in their areas of responsibility, the community needs one body that produces predictive intelligence estimates based on the entire community's gathered intelligence.

Strategic intelligence estimates highlight what may happen. They can help to direct a course of action that avoids a foreign policy misstep or allows the U.S. military to take a defensive posture to deter and mitigate the impact of an enemy attack. Strategic intelligence estimates also produce products that are research and context based. The information comes from a breadth of sources that provide a wider coverage of incidents unfolding around the world.

H. THE GRAY ZONE

Today, the U.S. Army Special Operations Command conducts activities in what is now called the "gray zone." According to the Special Operations Command, "The **gray zone** is a conceptual space between peace and war, where activities are typically ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet intentionally fall below the level of large-scale direct military conflict."[106] Activity in the gray zone is a purposeful action by an adversary to achieve a security objective by means that are ambiguous or that cloud attribution. Activities can involve the use of a single element or multiple elements of power. The activities are conducted by non-security domains or as part of a nation-state, but their overall purpose is to gain a security advantage against another actor. If an activity is attributed to the use of coercive force, the event is no longer a gray zone activity, but now subject to activities carried out in a traditional war battle space.[107]

---

[105] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 416.

[106] G. Popp et al., "Strategic Multi-layer Assessment (SMA) Panel Discussion on the Gray Zone in Support of USSOCOM" (panel discussion report, NSI, 2017), 12, http://nsiteam.com/panel-discussion-on-the-gray-zone/.

[107] Ibid., 12.

Threats in the gray zone are challenges to or violations of recognized international customs, norms, or laws. The purpose of the threat is to pursue a broad national security objective, but not to provoke a response from a nation-state's military force. A gray zone threat, which occurs in violation of international rules or norms, can arise in three ways.

The first way to create a gray zone threat is to challenge understood norms, though not in a fashion that violates international law. In 2014, Russia began a political warfare campaign with the strategic goal of acquiring Crimea. Russia used its instruments of power (military, intelligence, political agitators, and criminal elements) to disrupt Crimea's stability. Pro-Russian groups amassed in Crimea, and Russia took a military defensive posture on the Russia–Crimea border. Although funding for the activities has been associated with the Kremlin, the activities have not been officially attributed to Russia.[108] The Crimea annexation occurred from within; Russians were placed within the Crimean population. These actors were then able to pursue Russian strategic objectives by influencing people's perceived needs and decision making in a way that favored Russia.[109]

The second way to create a gray zone threat is through violations of international norms, but in a manner that avoids legal penalties (i.e., actions that do not technically violate laws, and therefore do not warrant punishment). In 2016, China began a strategy of border expansion by extending its maritime borders, infringing on the recognized United Nations Convention on the Law of the Sea. To make its claims, China asserted "island reclamation" to expand its borders to the South China Sea, citing physical structures as claims to extending sea borders.[110] Extending boundaries into the South China Sea would give China a strategic advantage in a highly valued trade route.

---

[108] U.S. Army Special Operations Command, *SOF Support to Political Warfare* (Fort Bragg, NC: U.S. Army Special Operations Command, 2015), 4–5.

[109] Special Operations Command, *Perceiving Gray Zone Indicator*, 8.

[110] John A. Stevenson, Belinda Bragg, and Sabrina Pagano, *Violating Normal: How International Norms Transgressions Magnify Gray Zone Challenges* (Arlington: VA, Strategic Multi-Layer Assessment, 2017), 4.

Finally, a gray zone violation can occur when violent extremist organizations or non-state actors apply use of force or power to achieve a security interest.[111] In 2011, the world saw the re-emergence of Da'esh, also known as the Islamic State, in the Iraqi and Syrian regions. By June 2014, Da'esh leader Abu Bakr al-Baghdadi announced the formation of a caliphate encompassing land in both Syria and Iraq. To secure its land, Da'esh began its own organized battles to defeat local military forces and took control of Fallujah (Iraq) in December 2013 and Raqqa (Syria) in January 2014. After a bloody month in September 2014, as the world watched public beheadings of journalists and aid workers, the United States formally declared a military campaign, Operation Inherent Resolve, to combat Da'esh.[112]

Traditional U.S. military operations have focused on a battle space in which another state is the clearly identified opponent.[113] The United States' last official declaration of war occurred in 1941; more recently common is participation in foreign military operations, or informally declared wars. The engagement of U.S. military operations in a foreign setting is more representative of strategic strikes than the large-scale responses traditionally associated with declarations of war.[114] The traditional nation-state has been the acknowledged government body in international negotiations; new challenges, however, include non-state actors and other sources of legitimized authority.

While the U.S. military is still a leading force on the world stage, entry into gray zone activities is limited to the areas that directly challenge U.S. security and its interests. Inflexible, centralized decision making and a lack of a unified government response hamper U.S. gray zone operations.[115] To meet the new challenges in an evolving

---

111 Stevenson, Bragg, and Pagano, *Violating Normal*, 12.

112 Cameron Glenn, "Timeline: Rise and Spread of the Islamic State," Wilson Center, July 5, 2016, https://www.wilsoncenter.org/article/timeline-rise-and-spread-the-islamic-state.

113 Special Operations Command, *The Gray Zone*, 1.

114 Ibid., 3.

115 Ibid., 5.

operational environment, the U.S. military moved away from a traditional war response and began to consider operations that aligned with the current security threat.

In pursuing this course of action, the Special Operations Commands began to examine best operation practices for this new battle space, taking a more abstract approach.[116] First, they recognized that there was no "win" in gray zone activities; the objective is positional advantage for the U.S. government. To gain this advantage, they realized the need to employ capabilities that influence parties in the operational environment, such as regional partners, local populations, and those posing threats to U.S. strategic objectives. Rather than accomplishing objectives through the sheer use of force, Special Operations Command is gaining the advantage in the cognitive decision space by influencing others to meet U.S. strategic objectives and denying adversaries the opportunity to have influence or to take action.[117]

Intelligence today must include continuous monitoring that analyzes the value of information obtained and determines how the information informs the intelligence community during emerging events.[118] When Cold War indicators no longer met the intelligence community's needs, the community began gathering information from newly developed technologies like satellite imagery, electronic intelligence, and geospatial intelligence.[119] Michael Handel argues that this approach leaves the intelligence community vulnerable to surprise and does not account for the role of human interaction in intelligence.[120] National security policies today need to reflect population-centric strategies that account for the impact of sociocultural elements in an operational environment or global region.[121] To meet this growing need, the Special Operations

---

116 Special Operations Command, *The Gray Zone*, 7–8.

117 Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80, no. 1 (2016): 108, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

118 William J. Lahneman, "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (2010):, 209.

119 Michael I. Handel, "Intelligence and the Problem of Strategic Surprise," *Journal of Strategic Studies* 7, no. 3 (1984): 235.

120 Ibid., 235.

121 Tomes, "Toward a Smarter Military," 70.

Command has recognized its new battle space in the human domain, and the necessity to understand how to maneuver in this space to meet U.S. objectives.[122]

[122] U.S. Special Operations Command, *Operating in the Human Domain*, Version 1.0 (MacDill Air Force Base, FL: U.S. Special Operations Command, 2015), http://nsiteam.com/social/wp-content/uploads/2017/01/SOF-OHD-Concept-V1.0-3-Aug-15.pdf.

III. ADAPTING GRAY ZONE INDICATORS

A. THE HUMAN DOMAIN

In 2015, the U.S. Special Operations Command developed the "operating in the human domain" concept, which calls for a change in mindset to achieve strategic goals in present and future operational environments.[123] According to the Special Operations Command, the human domain comprises "people (individuals, groups and populations) in the environment, including their perceptions, decision-making, and behavior."[124] In the human domain, the actors' values and beliefs—including political aspirations, perceptions of inequality, the state of the economy, or feelings of injustice—shape the operational environment; understanding the actors allows the Special Operations Command to gain strategic influence.[125] "Success in the Human Domain depends on an understanding of, and competency in, the social, cultural, physical, informational, and psychological elements that influence human behavior."[126]

1. Framework for the Human Domain

The human domain encompasses five elements: social, cultural, physical, informational, and psychological. The social element is characterized by the capacity to influence key relationships, members of society, and institutions. Work in this element involves different persons or groups—such as local governments or societal groups and civic groups—attempting to gain influence over others. Social power can take many forms, but usually relates to the vastness of the actor's network and the strength of his or her connections to those in the network. Social power also relates to the breadth and quality of the information that is available to the actor.[127]

---

[123] Special Operations Command, *Operating in the Human Domain*, 3.

[124] Ibid., 3.

[125] Ibid., 15, 23.

[126] Ibid., 3.

[127] Ibid.,13.

The cultural element explains a people's behavior based on their customs, beliefs, and way of life. Cultural differences can contribute to how a person perceives an action or reacts to an activity. For example, one culture may accept the slaughter of an animal as an honorable practice, while another culture may view the same activity as shameful. Although there are many similarities among cultures, differences can be implicit or readily apparent, and these differences are definitive. A sampling of the cultural element includes ideology, religion, language, and customs.[128]

The physical element prioritizes needs, shapes a person's values, or dictates a person's behaviors. In evaluating the physical element, analysts consider how a region's physical elements can affect its inhabitants. For example, farmers in one region may find grass to feed their livestock a priority, while farmers in another region may value water to grow vegetables. Physical elements can include geography, hydrology, availability of resources, or the climate. The element that an actor values most will prioritize the physical need.[129]

The human domain's informational element includes potential sources of information and the availability of that information to the population. It also includes the transmission of information through different methods and transmission paths. In an urban area, information can easily be transmitted through traditional television broadcasts or sent through social media and repeatedly forwarded by the end user. In a rural or primitive area, information may be more commonly transmitted during group gatherings or through distributed leaflets. Analysts focusing on this element also evaluate the openness or restrictiveness of information disseminated by the government or other censoring body. The informational element can include use of the Internet, radio, spoken word, or other messages delivered to the population.[130]

The psychological element examines how information influences a person or group's actions, or the audience's perception and reaction. For example, someone who is

---

[128] Special Operations Command, *Operating in the Human Domain*, 13.

[129] Ibid.

[130] Ibid.,13–14.

religious may react differently to news of death than an atheist. In another example, citizens may react differently when a small town announces construction of a new shopping mall. Some may perceive that the town is becoming progressive, and that business will bring employment opportunities; others may believe the shopping mall will ruin the way of life for the small town residents. Analysis of the psychological element takes perception, reasoning, and emotion into account.[131]

The Special Operations Command has adopted gray zone indicators to track changing conditions and emerging events that could influence the operational environment. The indicators monitor a broad spectrum of activities beyond military maneuvers and activities along supply lines. Gray zone indicators help analysts take a more holistic approach, incorporating information about a region's social, cultural, physical, informational, and psychological elements. The activities monitored are not limited to those of a nation-state or state-sponsored actors. Because different regions will perceive information differently, analysts must also gather regional perspectives.[132] For example, a region with an established government and stable economy will signal different measures of change than a region that is experiencing insurgent warfare and a migrating population. While the indicators themselves do not change, it is important to understand which ones are relevant based on the region's makeup and its nuanced changes.

Warnings in the gray zone let the Special Operations Command know when an operational environment is becoming unstable, which is signaled in several ways. First, when U.S. strategic interests conflict with a gray zone competitor's interests, the situation can create tension. Second, tension can also arise when the United States' and its partners' key interests conflict with the interests of a gray zone competitor. Regional instability can also come from a gray zone competitor whose domestic motivations do not align with the United States' or its partners' interests. When these situations arise, the

[131] Special Operations Command, *Operating in the Human Domain*, 13–14.

[132] Ibid., 64–65.

command works to identify the tension-causing activities and develops a worst-case scenario for strategic or regional stability.[133]

2. Warning

Special Operations Command analysts search the five elements of the human domain for context-specific warnings of action. These warnings are evaluated based on the actor's motive, the conditions that can move the actor to take action, the opportunity to act, the triggers that set action into play, and the momentum to facilitate carrying out the act.[134] More specifically, when Special Operations Command analysts review information and intelligence for indicators in the gray zone, they:

- look for signs that an actor has new or changing motives, or may act on motives.[135]
- "apply multidisciplinary lenses to study the conditions in the operational environment, evaluating the potential energy between the mix of motives and conditions."[136]
- look for opportunities through which can actor may gain a positional advantage.[137]
- "measure the concentration of triggers indicating the direction and magnitude of an actor generating momentum."[138]
- calculate the actor's momentum along a potential trajectory to determine the appropriate zone in which to alter the condition and change the trajectory .[139]

The premise for these warning signals is the assumption that the actor (person) is the key security challenge in the human domain and will act to carry out non-normative interests. When the actor meets his threshold for capacity to act, he will act on his

133 G. Popp et al., "SMA Panel Discussion on the Gray Zone," 4.

134 Special Operations Command, *Perceiving Gray Zone Indicators*, 13.

135 Ibid., 13–14.

136 Ibid.

137 Ibid.

138 Ibid.

139 Ibid.

motives. The drivers of these motives subsist in ideological, economic, value, and power interests.[140] The pretext for action is the presence of an opportunity to pursue or initiate an action. Examples of these opportunities include legal actions, growing economic tensions, or socio-political disorder. The context of the condition can create momentum, triggering the actor to carry out his motives. These triggers provide insight into the actor's pursuit of his interests, whether by cognitive maneuvering, influence from morals, or physical movements that lead to a security challenge.[141] In the gray zone, warning signals expand from traditional military indicators. Threats to U.S. interests can come from criminal enterprises, non-state actors, operations that negatively frame the activities of the U.S. government, subversion by political bodies, coercion to deter activities, or an attempt to manipulate U.S. activities.[142]

In order to recognize warning signals in the gray zone, analysts must go beyond gathering intelligence alone. They must analyze various factors to determine if ongoing activities are connected; information gathering provides a fuller picture of what, if any, changes are forthcoming. Indirect signals in the operational environment may cue a coming change. No one-size-fits-all list of indicators exists; events must be continuously monitored to validate perceived changes in the operational environment.[143] Strategic warning in the gray zone requires awareness about the opportunities for non-standard campaigns and non-state actors.[144]

The role of strategic warning in the gray zone is to facilitate preemptive action before there is a surprise. Intelligence for conducting activities in the gray zone is distributed from an integrated intelligence structure, as outlined in the Joint Chiefs of Staff's Joint Publication 3-13, Information Operations.[145] Analysts collect and analyze

---

[140] Special Operations Command, *Perceiving Gray Zone Indicators*,12.

[141] Ibid., 12–13.

[142] Ibid., 11.

[143] Ibid., 14.

[144] Ibid., 1.

[145] Joint Chiefs of Staff, *Information Operations*, Joint Publications 3-13 (Washington, DC: Joint Chiefs of Staff, 2014).

information through a joint intelligence support element that includes areas like terrorism/weapons of mass destruction analysis, information operations support, collection management, and the work of a national intelligence support team.[146] An information operations cell focuses on the integration of cognitive, physical, and informational dimensions of intelligence collected to support operational activities.[147] This helps analysts develop an understanding of the operational environment from a human-centric perspective.[148] By collecting and monitoring advantageous indicators, analysts can reveal new risks to security over time. Strategic maneuvering in the gray zone anticipates the potential trajectories of gray zone challenges and provides a forward-looking warning.[149]

3. Measurements and Sources

The Special Operations Command continuously evaluates the operational environment through environmental analysis and assessment. This process gauges political, social, cultural, economic, and security trends within the operational environment. The analysis measures effectiveness by examining how those in the operational environment perceive the command's activities, determining if there is an impact on local decision making, and evaluating the behavior of identified actors. The process also includes a review of second- and third-order effects of the command's activities.[150]

The overall purpose of the environmental analysis and assessment is to inform the command about "how to engage" in the human domain. The process identifies relevant actors who are influencing the operational environment, as well as partners or those who will support the command's activities. This analysis allows command staff to evaluate

146 Joint Chiefs of Staff, *Information Operation*., II-10–11.

147 Ibid., ix–x.

148 Ibid., II-10

149 Special Operations Command, *Perceiving Gray Zone Indicators*, 5.

150 Special Operations Command, *Operating in the Human Domain*, 66.

active engagements and, if necessary, redirect activities or resources.[151] The assessment also gathers information from other U.S. military sources and partner nations.[152]

The analysis expands on traditionally utilized threat-based intelligence products. Beyond areas in the traditional threat matrix, analysts review political, military, economic, social, informational, and infrastructure elements for changing conditions and dynamic situations. The purpose of this expanded analysis is to understand the networks that threaten a nation through its vulnerabilities, and to determine how to gain influence over the population.[153] Analysts begin to model and analyze the environment by examining the following elements: level of security in the region or country, the accessibility and influence of technology, economic stability, political stability, availability and utilization of energy resources, overall social conditions, and the impact of the physical environment.[154]

To develop a strategic assessment of an operational environment, the Special Operations Command analyzes various sources. Though this list is not exhaustive, some techniques include social network analysis, sentiment analysis, advanced target audience analysis, and open source reporting. Social network analysis helps identify relationships between actors and visualize the influence actors have in a specified area. Sentiment analysis measures how a population perceives its government's intentions and capabilities by identifying popular and influential figures, like violent extremists, or the population's continued trust in the legitimate government. When engaging in advanced target audience analysis, analysts or trained academics collect information about host nations through polls. Finally, open source reporting draws on multiple sources of information to examine a region or nation's socioeconomic trends.[155]

---

[151] Special Operations Command, *Operating in the Human Domain*, 70–71.

[152] Ibid., 68.

[153] Ibid., 66.

[154] Ibid., 67.

[155] Ibid.

4. Making the Assessment

In the human domain, analysts assess potential security challenges by evaluating information, analyzing gathered intelligence, and tracking activities in the operational environment. They use both context clues and algorithms to assess actors' motives, the operational environment's conditions, and the momentum of the activities monitored.[156]

The military uses data and algorithms cautiously; they acknowledge that understanding the data collection methods and the algorithm outputs is of greater importance than the algorithm itself.[157] While algorithms help analysts distinguish trends, it is equally important to recognize what is driving a trend or the intervening variables that explain or connect trends.[158] One algorithm used by the U.S. Army Special Operations Command is the Community Detection Algorithm, which examines relational datasets and searches for subgroups that could be connected. The algorithm reports a modularity score, which correlates to the subgroups' cohesiveness through elements such as social connections or physical ties. To understand the groups' interconnectedness, however, analysts must examine the groups more deeply to interpret the algorithm results.[159] The U.S. Army Engineer Research and Development Center uses another algorithm, called STRIDER, to perform entity detection and identify resolution solutions. STRIDER provides analyzed datasets that tag people, the organizations they belong to, events occurring, and locations. The final product allows the analyst to see relationships through geospatial and networking tools.[160]

The Special Operations Command collects a wide variety of information and intelligence to understand the operating environment in the gray zone. Information is collected from various sources, including the State Department, regional field human intelligence from the battlefield, and a range of open sources. Information and

---

156 Special Operations Command, *Perceiving Gray Zone Indicators*, 13.

157 U.S. Special Operations Command, "SOCOM SMA Multi-agency Gray Zone Conversation (I&W Focused)" (briefing, U.S. Special Operations Command, 2016), 40.

158 Ibid.,43.

159 Ibid., 44.

160 Ibid., 50.

intelligence are gathered and analyzed through a multi-disciplinary lens to produce a broad view of the operating environment. This same analysis also helps the military determine how to best approach those occupying the operational environment. The indicators in the gray zone are then adapted for operations in a physical battle space in the human domain.

B. INDICATIONS FOR HOMELAND SECURITY

The U.S. intelligence community can incorporate the Special Operations Command's five evaluative indicators (or warning signals) into its activities. These indicators, described in more detail in this section, relate to motive, conditions, opportunity, triggers, and trajectory. Using these indicators will help shape a forward-looking intelligence estimate that can potentially lessen the probability of surprise. As with operations in the gray zone, all warning for the intelligence community will assume that the actor is the primary security challenge.

1. Motive

Indicator 1: *Look for signs that an actor has new or changing motives, or may act on motives.*[161]

For Indicator 1, the intelligence community will target an actor who they believe may have an impact on the operational environment. Actors are targeted for analysis based on their established networks and their ability to command those networks for personal use. The actor does not necessarily have to be a leader or prominent figure in the community; he could be a person who is vocal about his motives and is capable of communicating messages through his network, whether in person or electronically. The analyst must consider the actor's ability to take action on his motives and determine if those motives point to socially unacceptable or criminal activities.

An open-source search for the actor in Indicator 1 would reveal people at different levels of influence in a region or community. First, there are the traditionally expected leaders of government, educational institutions, militaries, public service entities, or

[161] Special Operations Command, *Perceiving Gray Zone Indications,* 13–14.

businesses. These sources often maintain a public social media presence that is well crafted and informative, and/or they have public websites. Outside of their official roles, these actors can also maintain personal social media presences that are open to the public, but much less formal.

A second level of actors are people known to the local region or the community because of the work they do—they could be known for raising awareness about issues, charities, or institutions, they could be hometown celebrities, or they could be known for the societal contributions they make. This type of actor also generally maintains a social media presence to keep others informed about their activities or to bring issues into the social consciousness. Their open-source presence likely includes a mix of professional and personal mediums, depending on their status (i.e., a local schoolmaster will have a different type of online presence than an advocate for saving the shoreline).

The third level is the individual actor who maintains a personal social media presence. This presence can range from activity on websites and other mediums that documents activities, are designed to push out information for public consumption, are informative and advocate for change, or offer guidance and advice on any number of topics. This actor can use this social media presence to put on a persona, which could paint him as a serious entrepreneur, an activist, a life coach, a religious servant, or even a self-proclaimed expert who is associated with an established organization or institution.

Actors identified by Indicator 1 will come to the intelligence community's attention through his activities, or through information and intelligence. The actor's relevance is based on how much his message and activities affect the U.S. government. If the actor's message advocates for activities that counter the U.S. government, analysts will work to determine the capacity of the actor's network and determine his target audience.

2. Conditions

Indicator 2: *"Apply multidisciplinary lenses to study the conditions in the operational environment, evaluating the potential energy between the mix of motives and conditions."*[162]

This second indicator calls for an assessment of the actor's motives and the factors that drive his motivation. This will require analysts to examine the social, cultural, physical, informational, and psychological elements to determine what is motivating the actor to move toward taking action (e.g., no employment, government raising taxes, etc.). The intelligence analyst must be cognizant of the actor's sociocultural environment to understand what is driving the actor's motives. Deeply engrained cultural values and customs guide the actor's behavior; assessing the actor's values (which can be ideological or economic, or related to value and power) will also help analysts determine potential motives or drivers. Because an actor's perceptions and reactions correspond to activities in his environment, the intelligence community should look for environmental conditions that couple with the actor's motives to fuel momentum for socially unacceptable or criminal activities.

Open-source data about famine, drought, and a region's health are available from sites like the World Health Organization's Global Health Observatory and the Food and Agriculture Organization of the United Nations.[163] While the actor identified by Indicator 2 may not readily present himself, other sources can reveal the state of the community. Migration patterns and livestock deaths, for example, are obvious signs of a poor environment. Additionally, in depressed regions of the world, aid workers often report back to their agencies about the communities in which they are working; the agency may then publish the information on its website. Opinion and editorial pieces in regional newspapers can also describe regional conditions and community feelings. Information can also come from local bloggers, from the perspectives of people posting on travel sites, and prayer requests from local communities or missionaries.

---

[162] Special Operations Command, *Perceiving Gray Zone Indications*, 13–14.

[163] For more information, see www.who.int/gho/en and www.fao.org.

3. Opportunity

Indicator 3: *Look for opportunities through which can actor may gain a positional advantage.*[164]

For Indicator 3, the intelligence community must search the operational environment for activities or incidents that can provide the actor with an opportunity to action. By reviewing local, regional, and ongoing activities, analysts can point to changes in the environment. These activities can include public social gatherings, political ceremonies, protests, pilgrimages, sporting events, and candlelight vigils. Actors will eventually seek opportunities to conduct socially unacceptable or criminal activities and gain strategic advantage; they may do so, for example, by causing a disruption, calling out a political figure in a public forum, or revealing unwanted activities on social media.

The actor relevant to Indicator 3 may not reveal himself quickly, but his opportunities to act are often announced publicly by the government, or in local newspaper announcements, social media, and television or radio broadcasts. Official sources inform the public about government and social activities in the community; it is during these activities—when the public and media will have no choice but to acknowledge him—that the actor will seek positional advantage. Examples of events that turn into opportunities include a terrorist who sets off a bomb during a concert, protesters who disrupt a government official giving a speech in a public location, or an actor setting fire to voting locations throughout a jurisdiction.

4. Triggers

Indicator 4: "*Measure the concentration of triggers indicating the direction and magnitude of an actor generating momentum.*"[165]

To act on Indicator 4, analysts must evaluate an actor or group's activities that point to escalating rhetoric or calls for action. The intelligence community should examine the actor's physical environment for conditions—or triggers—that may cause

[164] Special Operations Command, *Perceiving Gray Zone Indications*, 13–14.

[165] Ibid.

the actor to conduct socially unacceptable or criminal activities, such as anger or frustration that may cause the actor to seek change in his environment. Analysts should also heed the reactions of the larger group that the actor can influence with information or activities.

For Indicator 4, the actor's social media presence is the best source to examine for concentrated triggers. Social media activities—such as postings on a personal page, postings the actor has written to others, and posts to which the actor has responded or engaged in dialogue—can illuminate the actor's emotions, reasoning, and intentions, and can show what the actor has asked others to do or support, including through financial assistance.

The actor's momentum is measurable in several ways. First, examining the actor's social media pages for "likes," comments, and "shares" will reveal those who agree or disagree with his message. A social media review would can also provide a rough estimate of the actor's base social network. Analysts can also crowd source for opinions about the actor's thoughts and ideas to determine the general level of support the actor is receiving from his audience. Additionally, a social network analysis could show the strength of the actor's network, as well as the vulnerabilities for disrupting his network.

5. Trajectory

Indicator 5: *Calculate the actor's momentum along a potential trajectory to determine the appropriate zone in which to alter the condition and change the trajectory.*[166]

Working with this final indicator involves assessing the regional environment and evaluating the threats for non-normative behavior expressed by an actor. Along with evaluating the threats themselves, analysts must identify the resources available to modify the actor's behavior or change the environment to favor U.S. interests. An assessment can also determine the instruments of power the United States can utilize in the emerging situation to change the trajectory of the actor's non-normative actions.

[166] Special Operations Command, *Perceiving Gray Zone Indications*, 13–14.

Indicator 5 provides a snapshot of the region and the actor to estimate the actor's course of action and to take measures to thwart him. The Special Operations Command has recognized that operations in the human domain succeed when they anticipate needs, general sentiments, and adversaries in the operational environment. When there is a threat of non-normative behavior, they must take action to change the direction of that behavior in favor of the United States.

The U.S. intelligence community should be evaluating regions of the world to anticipate non-normative behavior that can guide foreign policy. Related analyses should heed the region's sociocultural state and the triggers that are pushing actors to participate in non-normative activities. Foreign policy decisions should then be based on the appropriate course to ensure the direction of any activity is in favor of the United States. Continuous monitoring will allow the community to better understand how small regional changes may impact U.S. interests, and will help the community better prepare for impending changes in regional stability.

C. DEVELOPMENT OF MODERN INDICATORS FOR HOMELAND SECURITY

The U.S. Army Special Operations Command uses a process known as environmental analysis and assessment to determine how to engage with actors in its operational space. This measure also correlates with the Political, Military, Economic, Social, Informational, and Infrastructure threat matrix. Collected data is processed through algorithms designed for military use, to address a military problem set. The Special Operations Command incorporates information from social network analyses, sentiment analyses, and target audience analyses to produce a holistic picture of the operational environment. Information gathered by the Special Operations Command and other military partners also becomes part of the overall analysis.[167] The analyzed information helps the military make informed judgments about its operating environment, actors that should be monitored for non-normative activity, and general threats to environmental stability.

[167] Special Operations Command, *Operating in the Human Domain*, 66–71.

Although the Political, Military, Economic, Social, Informational, and Infrastructure threat matrix was developed for military use, its use is not limited to combat operations. It identifies areas where it will be necessary to conduct work, but does not explain how military activities should be conducted in the operational environment.[168]

A modern warning indicators matrix for homeland security can be modeled after the Special Operations Command's threat matrix. This proposed warning indicator matrix (shown in Table 1) provides analysts with a broad view to anticipate future events precipitated by an actor in the present environment. The social, cultural, physical, informational, and psychological elements form the columns along the top of the matrix. The indicators form the rows along the left side of the matrix. The actor is the key security challenge in the environment, and the indicators reflect the actor's activities. The actor can be an individual, a group, an institution, or any entity that can move an operational environment away from the strategic interests of the United States.

168 R. Hillson, "The DIME/PMESII Model Suite Requirements Project," *2009 NRL Review*: 235, https://www.nrl.navy.mil/content_images/09_Simulation_Hillson.pdf.

Table 1. Modern Indicators Matrix

ELEMENT	Social	Cultural	Physical	Informational	Psychological
INDICATOR					
Motive					
Conditions					
Opportunity					
Triggers					
Trajectory					

The elements along the top row of the matrix (described in more detail in Table 2) are the same elements the Special Operations Command uses to understand its operational environment. Learning how these elements influence the region or area where activities are conducted gives a perspective on how each element shapes the population and is valued by those in the region. It also helps indicate how changes in these elements can alter the regional environment. For each element across the top of the matrix, an actor indicator must be evaluated. This provides a broader perspective of what elements in the region can influence an actor and ongoing activities, changes, or opportunities that can trigger activity.

Table 2. Modern Indicators: Elements

Social	**Cultural**	**Physical**	**Informational**	**Psychological**
• Key relationships • Society • Institutions	• Behavior based on customs • Beliefs • Way of life	• Prioritizes needs • Shapes values • Dictates behavior	• Potential sources of information • Availability of information to the population	• How information influences the actor's actions • Audience perception of and reaction to information received
Relation to: • Actor's network • Strength of connections • Breadth and quality of information available	*Relation to:* • How an actor perceives an action • How an actor reacts to an activity or action	*Relation to:* • How physical elements affect inhabitants (e.g., food, water, resources)	*Relation to:* • Methods of information transmission • Paths for information transmission	*Relation to:* • Perception • Reasoning • Emotional response

The indicators in the first column of the matrix (described in more detail in Table 3) are the same indicators the Special Operations Command uses. The actor is the key security challenge and his non-normative interests are evaluated against each element. Understanding the actor's cognitive maneuvering in these elements can provide insight into what is moving the actor toward undesirable activities, and can indicate why the actor is moving toward pursing a certain course of action. The matrix in Table 4 provides a sample of the elements and indicators combined into a full matrix.

Table 3. Modern Indicators: Actor

Motive	Who in the environment is advocating a change, wrong, grievance, etc.? What is the actor's capacity to act: is he charismatic, are others attracted to his message, can he organize a group, is there political power backing the actor, etc.?
Conditions	What is the potential energy between the actor's motives and the conditions to take action? What is driving the actor's motives (e.g., anger, huger, shelter, sick family member, frustration)? What in the environment is creating the condition to move the actor (e.g., rising food prices, lack of employment, lack of resources, insurgent fighting)?
Opportunity	What are the activities in the environment that provide the actor with the opportunity to take action (e.g., concerts, protests, political speeches, union meetings, food distribution center, travelling medical clinic, religious services, military movements)?
Triggers	Is there a concentration of triggers that are moving the actor to take action (e.g., failed governance and forced migration, lack of food and a call for higher taxes, schools abandoned and overtaken by insurgents)? Are these triggers being revealed and gaining in momentum (e.g., increased social media presence, calls for action by protests, calls to take up arms, calls to remove elected officials)?
Trajectory	What is the actor's anticipated non-normative behavior and how can his trajectory be changed?

Table 4. Modern Indicators Matrix Sample

	Social	Cultural	Physical	Informational	Psychological
Motive	Strong ties to religion Strong ties to family	Upset by perceived lack of respect for religious institutions	Lack of basic needs: food and water	Religious leader preaches that U.S. military is starving population	Believes that becoming a suicide bomber will save his family and honor his religion
Conditions that Move Actor	Family relates to religious leaders' statements	Feels family is mistreated by U.S. military	Parents are starving	Believes U.S. military is blocking food delivery to starve population	Sees suicide bombing as an honorable activity Believes websites that indicate suicide bombing is an honorable act
Opportunity to Act	Talks with friends about unworthy U.S. military	Anger at lack of care for occupying his land	Siblings are starving/ siblings' health is failing	Told location of U.S. military living quarters and continued preaching of unworthy U.S. military	Anger at perceived comfort of soldiers
Triggers to Act	Friends talk about becoming suicide bombers	Family not able to sustain itself by living off the land	Starvation and lack of potable water	Continued preaching that U.S. military is stopping resources from reaching region	Growing anger at U.S. military
Trajectory	Friends are enlisting as suicide bombers	Family cannot afford to buy food	Family starvation No water No food	Calls for action against the occupying U.S. military, increasingly calls on social media and town meetings	Becoming a suicide bomber is honorable and will allow his family to buy food

Possible Solutions to Change Trajectory:

1. Bring in non-governmental organizations for resources like food, water, and medication (have positive interaction)

2. Promulgate messages about the services available and the military's purpose in the region.

3. Do nothing.

Modern warning indicators for homeland security must incorporate a human-centric approach that recognizes the actor as the security threat. The human-centric factors can better explain how changes are occurring regionally, even when an immediate response is not required. In today's fast-paced, changing world, it necessary to analyze events at the regional level, without an expectation that signs of change will come from nation-states. The U.S. intelligence community must provide a broad intelligence estimate that takes into account the smallest nuances of change and how they may affect regional stability. Exploring the use of a human-centric indicator matrix will allow those who conduct intelligence activities to collect and examine information gained through a multidisciplinary lens that more comprehensively explores a region's human domain.

IV. APPLICATIONS FOR HOMELAND SECURITY

The U.S. Army Special Operations Command has leveraged a people-centric strategy to gain a strategic advantage in its human-domain battle space, which is defined by different operational environments. The U.S. intelligence community can no longer rely on an intelligence paradigm that has a known nation-state as an enemy, nor can the community rely solely on technological advances for intelligence collection. The community must incorporate a human-centric emphasis into today's intelligence products, especially considering the impact of the human dynamic in intelligence and operational planning activities. While technological advances have provided advanced intelligence collection and analysis techniques, the intelligence community has yet to emphasize the "hearts and minds" of people within the human domain, and how they can play a role in influencing the will, resolve, and activities of others.

In today's world of blogs, social media, and Internet connectivity, multiple sources can provide information on the human condition across the globe. From the simplest post—perhaps an innocent essay written by a child—to a well-developed manifesto, the human domain has been electronically captured on the Internet. Along with personal musings and informative insights into the workings of life, the Internet is a source of information on the rich cultural heritages around the world, the philosophies and traditions of ancient religions, and the bountiful histories of nations. These information resources are complemented by domestic politics and a changing international social landscape.

A. A SURVEY OF SOURCES TO DEVELOP MODERN INDICATORS

To use gray zone indicators for homeland security, analysts must assemble reliable and relevant information from open sources. The U.S. Army Special Operations Command uses several related assessment tools to understand a region or its residents, and to gain a strategic advantage or to change the trajectory of an event in favor of U.S. interests. A modern warning indicator framework for homeland security should concentrate similarly within the human domain, using the Special Operations

Command's system as a guide. The strategic intelligence product should include a component that considers the complex influences that shape individual and group behavior.

In a working environment, collecting intelligence is the responsibility of the investigating entity. Local information collection will help analysts reach a better understanding of the social environment where activities are taking place, through which they can gauge what dangers, threats, or hostilities exist in the local environment; identify actors of interest; and determine the sociocultural background of the people. For example, social and cultural activities in a large urban metropolis with a commuter community will be different from those in a medium-sized suburban community characterized by residential neighborhoods and an aging population. Intelligence collection for the same activities in both environments is possible, but the social, cultural, physical, informational, and psychological elements could be different. Like the operation of the Special Operations Command, embedded homeland security intelligence units need to operate within the area of interest to monitor activities for signals of change. These signals will then need to be evaluated to determine if a response or change in posturing is necessary, which is possible with an on-site intelligence analyst to give context to the indicators.

Analysts can assess the presence of modern warning indicators by searching for information among diverse publicly available sources. As with the Special Operations Command's gray zone indicators, homeland security warning indicators need to identify a wide range of socio-political and economic factors that also provide information relative to the security of a region or people, while simultaneously providing insight into the influence of cultural factors in the operational environment. Open sources that are publicly available on the Internet provide a wide variety of resources and information needed to initiate a modern warning indicator matrix. Some of the sources provide datasets, others include reports, and some conduct their own algorithmic analyses.

A sample of the available sociological and cultural information revealed several large data sources. The electronic Human Relations Area Files World Cultures website covers all aspects of cultural and social life, presented in ethnographic collections that are

searchable. The start for any informational search is available by using the Outline of Cultural Material thesaurus. The site provides cross-cultural databases and comprehensive topical summaries of cultures.[169] The Compendium monitors national cultural policies in Europe and aims to include all fifty member states that belong to the European Cultural Convention. Profiles for countries also include the nations' historical development, legal framework, and financial characteristics. The Compendium presents summaries for national profiles, culture-related projects (e.g., migrants and refugees), an intercultural cities index, cultural statistics in Europe, comparative and monitoring overviews, and monitoring standards in cultural policy (including developments and trends).[170] The Global Database of Events, Language, and Tone (GDELT) Project is a platform that monitors the global world, as an open dataset, and works toward making all of society "computable." The following datasets are available: news, television, images, books, academic literature, open web, and use of algorithms for simple matches to deep statistical modeling. There are also measures of emotions and themes according to the site's Global Content Analysis Measures and over 100 themes in the Global Knowledge Graph.[171]

When it comes to politics and policy, global agencies and watch groups collect data and conduct research, and post the results online. The Global Policy Forum independently monitors United Nations policy and evaluates global policymaking. The group's focus includes the environment and development concepts, politics, financing for development, tax justice, United Nations reform, global governance, corporate accountability, peace and security, and food and hunger. The Global Policy Forum is actively involved with international non-governmental organization networks, including Social Watch and the Global Alliance for Tax Justice.[172] World Politics Review is a nonpartisan organization that analyzes global trends and distributes a daily analytical product on its website, which is a five-minute read. In addition to a daily brief, the World

[169] For more information, see www.ehrafworldcultures.yale.edu.

[170] For more information, see www.culturepolicies.net.

[171] For more information, see www.gdeltproject.org.

[172] For more information, see www.globalpolicy.org.

Politics Review publishes New Wire, an aggregation of significant news stories. The site is searchable by world region and by any issue.[173] Similarly, the Pew Research Center conducts the Global Attitudes Project and maintains an interactive database. Key trends are accessible on a range of topics and sorting is available by question topic or country of interest. For its Global Attitudes and Religion and Public Life projects, the Pew Research Center conducts interviews in ninety-one countries and offers seven searchable datasets.[174]

There is also a group of Internet sites for global monitoring organizations. The World Health Organization's Global Health Observatory provides health-related statistics for its 194 member countries. The World Health Organization actively monitors healthcare systems and related corporate services, as well as communicable and non-communicable diseases; the organization also plays a role in preparedness for and response to health crises. The organization's website offers over twenty searchable databases for review.[175] The World Bank is an international financial institution that provides financial products and assistance to help countries innovate and foster solutions for financial problems. The World Bank offers a large searchable database, as well as research and publication products.[176]

Finally, there are a variety of websites that provide information about security. The Security Assistance Monitor is a project of the Center for International Policy. The site documents all publicly accessible information on U.S. security and defense programs around the world. Information includes arms sales, bases and deployments, training, and military and police aid, among other topics.[177] NightWatch is a daily newsletter patterned after U.S. government briefings. NightWatch commentaries cover more than twenty-five countries. They track and assess threats to national security using open-

[173] For more information, see www.worldpoliticsreview.com.

[174] For more information, see www.pewglobal.org.

[175] For more information, see www.who.int/gho/en.

[176] For more information, see www.worldbank.org.

[177] For more information, see www.securityassistance.org.

source information. The newsletters assess the impact of war, global internal instability, and terrorism.[178]

In early 2017, a new resource became available to search for gray zone indicators. Production of the U.S. Discoverable Government Information Assets Directory (US-DiGIA) brought together open-source information that was available throughout the U.S. government on non-Department of Defense and non-Office of the Director of National Intelligence websites.[179] The electronic directory provides unclassified information that is relevant to national security and foreign policy. The information comes from publicly available political and social information, data analysis, and subject-matter experts. The collated directory is easily searchable and, when possible, provides a point of contact for follow-up. The directory searches open sources of information for application to gray zone operations on different levels, like actor or rule violations.[180]

The US-DiGIA can be further mined for specific information; for instance, information gained from U.S. government sources could be categorized by determining: (1) what type of information is available, (2) who collects (and retains) the information, and (3) where the information is focused (geographically). The result of this data mining revealed 1,900 individual information assets across twenty-one organizations in the executive branch of the U.S. government.[181] Discoverable information assets fell into the following categories: economic, diplomatic, governing, law enforcement, physical environment, financial, security, information, intelligence, social, military, cyber, infrastructure, and twenty-three other assets that remain uncategorized.[182] One issue of note was the lack of clear geographically defined areas among the information assets. Also, none of the assets for intelligence, military, or cyber could be geographically

---

[178] For more information, see www.kforcegov.com/products/nightwatch.

[179] Sabrina J. Pagano, *US-DiGIA: Overview and Methodology of U.S. Discoverable Government Information Assets Directory* (Arlington, VA: Strategic Multi-layer Assessment, 2017), http://nsiteam.com/social/wp-content/uploads/2017/07/Mapping-Methods-Report-05-13-2017.pdf.

[180] Ibid., 1–2.

[181] Belinda Bragg, *US-DiGIA: Mapping the USG Discoverable Information Terrain* (Arlington, VA: Strategic Multi-layer Assessments, 2017), 4, http://nsiteam.com/social/wp-content/uploads/2017/07/Mapping-Methods-Report-05-13-2017.pdf.

[182] Ibid., 6.

defined from the discoverable sources.[183] The directory is simply an information resource that begins to work toward a whole-of-government approach by gathering very different resources into one information hub.[184] The current information does not provide direct indicators for warning in the gray zone; however, it does contain information that could potentially assess an actor's vulnerability in the gray zone, as well as information pointing to physical environments that may be developing into gray zones.[185] What this directory does provide is an information resource that catalogs the levels of expertise in the U.S. government that can contribute to producing broader national security strategies.[186]

B. INCORPORATING A HUMAN-CENTRIC INTELLIGENCE APPROACH

The U.S. Army Special Operations Command developed gray zone indicators to better gauge the operational environment in their battle space. These indicators warn of non-normative behaviors that are potentially harmful or criminal, and emerging threats. They also provide an overview of the cultural and social customs that are most important while engaging in a region. Gray zone indicators can also direct attention to persons who may become partners in achieving U.S. goals by moving the trajectory of an event in favor of U.S. objectives.

The Special Operations Command's use of gray zone indicators is a model for homeland security practitioners to incorporate a human-centric approach into their intelligence activities. The social, cultural, physical, informational, and psychological elements measured against the indictors of an actor in an operational environment provides a matrix by which the U.S. intelligence community can change an actor's trajectory in favor of the United States. Application of a modern indicator matrix using human-centric indicators can help the intelligence community understand how conditions are changing in different regions of the world. Use of the matrix focuses on how an actor

183 Bragg, *US-DiGIA*, 12–13.

184 Ibid., 3.

185 Ibid., 22.

186 Ibid., 25.

can influence change in the environment, and the factors that can change a region. When these changes are detected, they signal an event on the horizon. This allows the intelligence community to evaluate the changing circumstances and decide if, and how, the United States should be prepared to thwart the trajectory of a threat or simply monitor a situation as it develops. A sample list of information that can translate into possible indicators is shown in Table 5.

Table 5. Possible Indicators for Homeland Security

Social	• Has social media activity increased? • Where are people gathering and for what purpose? • What is trending on social media sites? • Is there a call to action against a target on social media and what is the general feedback?
Cultural	• Sentiment analysis • Crowd sourcing • Changes in demographics • Changes in cultural activities (church, municipal celebrations) • Published opinion or editorial pieces and blogs
Physical	• Employment opportunities and unemployment rate • Housing availability • Food prices and availability • Healthcare crises and access to medical facilities
Informational	• Notable speakers and visitors (invited or presented themselves) • Where Internet users are being directed during searches • Increased activity on the dark web • Focused narratives being messaged through different mediums
Psychological	• Are people responding to calls for action? If so, what is being suggested? Is criminality of action increasing? • Is there an increase in purchase of harmful instruments (guns/knives)? • What is the emotional response (political activity, response to government action, reaction to local/regional event)?

C. HOMELAND SECURITY APPLICATION EXAMPLES

A modern indicator matrix that draws on human-centric sources of current information can help provide a forward-looking intelligence estimate. Continuous monitoring of local, regional, and national events provides a broad overview of what is happening in a state, while at the same time allowing analysts to monitor local and regional areas that can be the cause of instability. This broader geographic picture gives the U.S. intelligence community a method for monitoring activities and gathering information in different geographical areas. This information can then help to determine if the activities have a common cause or may result in instability, or if the United States should start preparing for the use of its instruments of power.

A human-centric matrix that considers sociocultural factors can help analysts quickly identify political actors in an operational environment. Identifying potential actors and understanding those actors' ability to influence others can inform the U.S. intelligence community about the possibility of an emerging situation and can provide an estimate of the number of people likely to become involved. Determining key actors in an operational environment can also help to establish their motives. With this information, the intelligence community can begin to evaluate options for threat mitigation, like passing on the information to the military or other authorities. Once an actor is identified, analysts can then determine the activity the actor is likely to pursue, such as a peaceful protest or a call to arms.

Conducting intelligence activities using a human-centric modern indicator matrix can provide the needed estimative intelligence about possible opportunities to act. After the actor has been identified and motives determined, those in the intelligence community can then begin to look for opportunities to counter the actor's motives. If the actor is unknown, then the opportunities for action and motives to act can be evaluated to look for a possible actor. Rather than maintaining a continuous state of anxious readiness, a directed effort can be made to identify the actor's target and put protective measures in place or stop the threat. Focus can remain on the opportunities to act while analysts also evaluate triggers in the operational environment. Looking at the conditions that are driving the actor, the operational environment should be monitored for a rise in tensions

around the driving conditions, like shortages of basic food needs or a divisive political speech followed by legislation that is perceived to be oppressive.

Taken as a whole, these human-centric indicators can help the U.S. intelligence community identify potential actors in an operating environment and better understand what drives them. Focusing on the actor's motives and possible triggers that may cause the actor to take action will help warn analysts about a possible event on the horizon. The intelligence community can then work to inform decision makers about the conditions driving the actor and the possible trajectory of actions.

The human-centric indicator matrix is not limited to intelligence gathering outside of the United States; it can have direct application in the domestic intelligence environment. This same matrix can be adopted across regions of the country, by states, or even by large metropolitan areas like New York City. This matrix is also not limited for use by the intelligence community. It can apply to any operational environment (a neighborhood, tri-state region, or a city business district). The operational environment is determined by the user, but the indicators remain consistent and so do the elements against which they are evaluated.

1. Net Neutrality: An Example of Environmental Monitoring

In 2015, the Title I of the Communications Act removed the Federal Communications Commission's (FCC's) authority over Internet service provider activities. This net neutrality act stated that websites could not be selectively blocked by Internet service providers, selectively chosen sites could not be slowed down, and selected sites could not be asked to pay more for better quality in service and faster speeds. The current FCC chairman, Ajit Pai, is actively working to dismantle the net neutrality safeguards currently in place. To fight to maintain net neutrality, large Internet companies like Google, Netflix, and Kickstarter participated in the "Internet-Wide Day of Action to Save Net Neutrality" to show support for the rules in place. There have also

been online petitions and advocacy groups like Free Press and Fight for the Future that have supported maintaining net neutrality guidelines.[187]

Net neutrality is a divisive issue that has the potential to cause an actor to take malicious action. Many believe that access to the Internet is a fundamental right that the government should not infringe upon. As the net neutrality act is being dismantled, Internet activists may fight back by conducting cyberattacks against government institutions and others they believe are responsible for breaking down net neutrality safeguards. Cyberattacks for the cause of net neutrality can also have second- and third-order effects; for instance, the attacks could shut down e-commerce, sabotage the stock market, or hold the data of banking institutions for ransom. An attack can be as small as an actor releasing embarrassing personal files or photos, but attacks can also be as serious as stopping the functioning of a satellite. The issue of net neutrality is a concern at the national level and should be monitored closely, especially when court rulings and committee hearings take place. The chart in Table 6, and the possible solutions that follow, shows how the modern indicators matrix could be applied to the possible fallout of net neutrality issues.

[187] Jeff Dunn, "Reddit, Netflix, Google, and Dozens of Other Tech Companies Are Protesting Trump's FCC Today—Here's Why," *Business Insider*, accessed November 2, 2017, http://www.businessinsider.com/net-neutrality-explainer-Internet-protest-fcc-ajit-pai-2017-7.

Table 6. Modern Indicators Matrix: Net Neutrality

	Social	Cultural	Physical	Informational	Psychological
Motive	Strong ties to Internet community	Belief that all Internet activity should be treated equally	Internet resources restricted	FCC argues against net neutrality and for FCC regulation	Believes that a loss of net neutrality will only be advantageous for big telecom companies
Conditions	Internet calls for petition, advocacy, and education	Feels net neutrality is being dismantled	Rollback of net neutrality rules	Court and committee meetings for and against net neutrality	Losing Internet freedom
Opportunity	Online Day of Action, online petitions, calls to govt. reps to stop FCC	Anger at potential loss of net neutrality	Physical protests at FCC offices	Believes government (FCC) is overreaching its authority	Anger at court rulings and government response
Triggers	Increasing Internet chatter discussing malevolent activities	Frustration at having no influence in govt. decisions	Conduct cyberattacks against FCC	FCC accuses net neutrality advocates of attack on FCC website	Growing anger and frustration
Trajectory	Meeting on dark web to plan cyber attacks	Doing something will draw attention to the cause	Do something to have some influence	Search for virus and bots for cyberattack	Need to do something to save net neutrality

Possible Solutions to Change Trajectory:

1. Set a future date and forum on net neutrality discussions to give those for and against neutrality an opportunity to present their argument outside of court and government committee settings (try to alleviate frustration and feeling of having no influence).

2. Start working in the dark web to look for actors showing sentiment to conduct a cyberattack and actively seek ways to conduct the attack, which may be targeting FCC Chairman Ajit Pai.

3. Do nothing.

2. NYC Subway Example

In 2017, the New York City subway, operated by the New York City Metropolitan Transportation Authority (MTA), had an awful year, highlighted by massive subway delays, track fires, and train derailments. There were numerous causes for the delays, including workers leaving tools on the track bed or failing to secure garbage that caused track fires, and an aging system in need of repair. While the system is melting down, neither New York City nor New York State is willing to take the lead to provide the much-needed funding for repairs. Cosmetic changes, like folding seats in subway cars, did not receive a positive response by the ridership and added to their frustration with the subway system.

The New York City subway system has a ridership of almost 6 million people per weekday.[188] It serves as a major transportation service that moves a variety of communities, including school children, those working in the financial district, service workers, and municipal employees. Severe damage to the subway system, or shutting it down completely, would bring New York City to a halt. It would be nearly impossible for every subway rider to drive, carpool, or even take a bus into the city. Parents would have to find alternative ways to get their children to school and workers would have to find a way to cross bridges and boroughs to get to work. The police department would have to handle vehicle congestion and flaring tempers while New York City leadership began planning transportation alternatives. The tourism industry would be affected as well; stranded tourists would be unable to get to the airports and visitors at airports would be unable to get to Manhattan. There would also be a loss of revenue from the tourism industry that would have a ripple effect on the food service industry, among others. The financial district would not be able to operate if employees were unable to work from alternative locations, which would ultimately affect the American stock market. Even more critically, ambulances would not be able to get to patients, and patients who receive regular treatments would be unable to get to their healthcare facilities. Congestion would also stop the food industry, the shipping industry, and package delivery services. The

[188] "Highest Figures since 1948,) MTA, April 18, 2016, http://www.mta.info/news-ridership-subway-new-york-city-transit/2016/04/18/highest-figures-1948.

New York City subway system is a local condition, but it can have a national and international impact. The chart in Table 7, and the possible solutions that follow, shows how the modern indicators matrix could be applied to the possible fallout of a New York City subway failure.

Table 7. Modern Indicators Matrix: NYC Subway

	Social	**Cultural**	**Physical**	**Informational**	**Psychological**
Motive	Strong ties to straphanger community	No reliable alternative transportation service	Lack of transportation to get to work and get around	Media and social media reporting subway failures	Frustration at poor transportation alternatives
Conditions that Move Actor	Online communities calling for action against MTA	MTA fixes cosmetic only, and are not fixing the system	Trapped in a faulty system and late to everything	No positive progress reported in media or MTA	Feeling oppressed by the MTA and stuck in a failed transportation system
Opportunity to Act	Online petitions and online discussion forums	Meet up with other riders to discuss MTA failures	Scheduled protests: Times Square and MTA headquarters Trains run all day, every day	Continued reporting of lack of safety, security, and reliability of system	Wasting money and not fixing the system that actor is still paying to use
Triggers to Act	Suggestions for disrupting the system	Believes petitions and protests are unheard	Not able to speak at MTA public hearing	15 Sept 17: explosive device partially detonates on London train	System is melting down and still no relief from MTA
Trajectory	Encouraged by online community to physically disrupt system	Disrupting system will force MTA to do something	Affected by seeing people stuck and injured—anger grows	Search for methods and materials to disrupt system Copycat of London explosive detonation	System is broken—destroy it and start again—build it better

Possible Solutions to Change Trajectory:

1. Start looking for negative messaging and actors proposing to physically disrupt system, or who are providing tactics on how to disrupt the system.

2. Work with media and MTA to balance messaging and ways to help MTA alleviate conditions.

3. Do nothing.

D. CONCLUDING COMMENTS

The U.S. Army Special Operations Command incorporated the use of gray zone indicators into its intelligence capabilities to better understand the human domain. Gray zone indicators use human-centric measures to understand how to change the trajectory of threats, and to discover the causes that drive the threats. Today, these same indicators can be adopted by the U.S. intelligence community to perform a human-centric intelligence analysis that focuses on the individual actor and what drives the actor to take unacceptable or criminal action. The sources of this information are readily available through the Internet, higher-learning institutions, public forums, and even through local community groups. A human-centric matrix can be used to assemble and evaluate information for the threats and to understand what drives a threat. It can help the intelligence community better monitor those threats. To meet the emerging threats, the intelligence community must adopt new operational methods to understand modern threats.

Indications and warnings in homeland security are in need of augmentation; the intelligence community must develop new ways to recognize signs in order to track and mitigate threats. In just the past month, an active shooter in Las Vegas and the use of a truck as a weapon in New York City resulted in a significant loss of life. There is still much work to do to develop a homeland security indications and warnings problem set that uses human-centric indicators to combat planning and movement for future attacks.

LIST OF REFERENCES

Borch, Fred L. “Comparing Pearl Harbor and “9/11”: Intelligence Failure? American Unpreparedness? Military Responsibility?.” *The Journal of Military History* 67, no. 3 (2003): 845–860. http://www.jstor.org.libproxy.nps.edu/stable/3397329.

Bragg, Belinda. *US-DiGIA: Mapping the USG Discoverable Information Terrain*. Arlington, VA: Strategic Multi-layer Assessments, 2017. http://nsiteam.com /social/wp-content/uploads/2017/07/Mapping-Methods-Report-05-13-2017.pdf.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and beyond*. Washington, DC: Georgetown University Press, 2013.

Davis, Jack. “Improving CIA Analytic Performance Strategic Warning.” Occasional paper, Central Intelligence Agency, 2002. http://www.dtic.mil/dtic/tr/ fulltext/u2/a526569.pdf.

———. “Strategic Warning: If Surprise Is Inevitable, What Role for Analysis?” *Kent Center Occasional Papers* 2, no. 1 (January 2003). https://www.cia.gov/ library/kent-center-occasional-papers/vol2no1.htm.

Gentry, John A. “Warning Analysis: Focusing on Perceptions of Vulnerability.” *International Journal of Intelligence and CounterIntelligence* 28, no. 1 (2014): 64–88.

Glenn, Cameron. “Timeline: Rise and Spread of the Islamic State.” Wilson Center, July 5, 2016. https://www.wilsoncenter.org/article/timeline-rise-and-spread-the-islamic-state.

Grabo, Cynthia M. *Anticipating Surprise: Analysis For Strategic Warning*. Bethesda, MD: Joint Military Intelligence College, 2002.

———. “The Watch Committee and the National Indications Center: The Evolution of U.S. Strategic Warning 1950–1975.” *International Journal of Intelligence and CounterIntelligence* 3, no. 3 (1989), 363–385.

Handel, Michael I. “Intelligence and the Problem of Strategic Surprise.” *Journal of Strategic Studies* 7, no. 3 (1984): 229–281.

Heidenrich, John. “The Intelligence Community’s Neglect of Strategic Intelligence.” *Studies in Intelligence* 51, no. 2 (2007): 15–26. https://www.cia.gov/library/ center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/ the-state-of-strategic-intelligence.html

Hillson, R. “The DIME/PMESII Model Suite Requirements Project.” *2009 NRL Review*: 235–239. https://www.nrl.navy.mil/content_images/09_Simulation_Hillson.pdf.

Hulnick, Arthur S. “Indications and Warning for Homeland Security: Seeking a New Paradigm.” *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (2005): 593–608.

Joint Chiefs of Staff. *Information Operations*. Joint Publications 3-13. Washington, DC: Joint Chiefs of Staff, 2014.

———. *Joint Intelligence*. JP 2-0. Washington, DC: Joint Chiefs of Staff, 2013. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

Kuhn, Ulrich, and Tristan Volpe. “Keine Atombombe, Bitte: Why Germany Should Not Go Nuclear,” *Foreign Affairs* (July/August 2017).

Kuok, Lynn. “While the World Sleeps, Myanmar Burns: The Latest Rohingya Crisis.” *Foreign Affairs*, September 28, 2017. https://www.foreignaffairs.com/articles/burma-myanmar/2017-09-28/while-world-sleeps-myanmar-burns.

Lahneman, William J. “The Need for a New Intelligence Paradigm.” *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (2010): 201–225.

Margolis, Gabriel. “The Lack of HUMINT: A Recurring Intelligence Problem.” *Global Security Studies* 4, no. 2 (2013): 43–60.

Miller, Bowman H. “U.S. Strategic Intelligence Forecasting and the Perils of Prediction.” *International Journal of Intelligence and CounterIntelligence* 27, no. 4 (2014), 687–701.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*, 1st ed.. New York: W.W. Norton, 2004.

Pagano, Sabrina J. *US-DiGIA: Overview and Methodology of U.S. Discoverable Government Information Assets Directory*. Arlington, VA: Strategic Multi-layer Assessment, 2017. http://nsiteam.com/social/wp-content/uploads/2017/07/Mapping-Methods-Report-05-13-2017.pdf.

Popp, G., G. Canna, B. Bragg, J. Stevenson, and L. Kuznar. “Strategic Multi-layer Assessment (SMA) Panel Discussion on the Gray Zone in Support of USSOCOM.” Panel discussion report, NSI, 2017. http://nsiteam.com/panel-discussion-on-the-gray-zone/.

Stevenson, John A., Belinda Bragg, and Sabrina Pagano. *Violating Normal: How International Norms Transgressions Magnify Gray Zone Challenges*. Arlington: VA, Strategic Multi-Layer Assessment, 2017.

Tomes, Robert R. “Toward a Smarter Military: Socio-Cultural Intelligence and National Security.” *Parameters* 45, no. 2 (Summer 2015): 61–76. https://ssi.armywarcollege.edu/pubs/parameters/Issues/Summer_2015/9_Tomes.pdf.

Turner, Stansfield. *National Intelligence Warning*, Director of Central Intelligence Directive 1/5. Langley, VA: CIA, 1979. https://fas.org/irp/offdocs/dcid1-5.html.

Tzu, Sun, and Samuel B. Griffith. *The Art of War*. London: Oxford University Press, 1971.

U.S. Army Special Operations Command. *Perceiving Gray Zone Indications*. Fort Bragg, NC: U.S. Army Special Operations, 2016. http://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf.

———. *SOF Support to Political Warfare*. Fort Bragg, NC: U.S. Army Special Operations Command, 2015.

U.S. Special Operations Command. *Operating in the Human Domain*, Version 1.0. MacDill Air Force Base, FL: U.S. Special Operations Command, 2015. http://nsiteam.com/social/wp-content/uploads/2017/01/SOF-OHD-Concept-V1.0-3-Aug-15.pdf.

———. "SOCOM SMA Multi-agency Gray Zone Conversation (I&W Focused)." Briefing, U.S. Special Operations Command, 2016.

Votel, Joseph L., Charles T. Cleveland, Charles T. Connett, and Will Irwin. "Unconventional Warfare in the Gray Zone." *Joint Force Quarterly* 80, no. 1 (2016): 101–109.. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

Wirtz, James J. "Indications and Warning in an Age of Uncertainty." *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (2013): 550–562.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

Zegart, Amy B. *Spying Blind*. Princeton, NJ: Princeton University Press, 2009.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California